Joint Doctrine Note 1-20

Joint Identity Activities

24 November 2020

Unclassified

PREFACE

1. Purpose

Joint doctrine notes (JDNs) examine problems and potential solutions to support joint doctrine development and revision. JDNs can bridge potential doctrine gaps. This JDN addresses how identity capabilities may be coordinated and integrated to create effects across all phases of an operation or campaign. It supplements current joint doctrine and provides context for identity activities across the competition continuum. This document was developed using current joint doctrine, procedures, and policy guidance. It socializes identity activities-related information and procedures in a non-authoritative document that commanders and staffs can use.

2. Application

The guidance in this JDN is not authoritative. If conflicts arise between this JDN and a joint publication (JP), the JP will take precedence for the activities of joint forces, unless the Chairman of the Joint Chiefs of Staff provides more current and specific guidance.

STUART B. MUNSCH
Vice Admiral, United States Navy
Director for Joint Force Development

Intentionally Blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY vii

CHAPTER I
OVERVIEW

- Introduction I-1
- Identity Activities I-4
- The Relationship Among Intelligence, Maneuver, and DOD Law Enforcement Units I-9

CHAPTER II
IDENTITY ACTIVITIES SUPPORT TO MILITARY OPERATIONS

- The Role and Placement of Identity Activities in Military Operations II-1
- Support to Military Operations Across the Competition Continuum II-2
- Planning Identity Activities II-5
- Planning Considerations II-8
- Capability Needs Across the Phases of an Operation II-11
- Additional Planning Considerations II-16
- Assessment of Identity Activities II-24
- Using Identity Activities to Support Operational Assessment II-25

CHAPTER III
IDENTITY ACTIVITIES CORE CAPABILITIES

- General III-1
- Biometrics III-2
- Forensics III-4
- Document and Media Exploitation III-7
- Identity Intelligence and Criminal Intelligence III-8

CHAPTER IV
SPECIAL CONSIDERATIONS

- General IV-1
- Authorities IV-1
- Legal and Policy Considerations IV-3
- Multinational Operations IV-9
- Sharing of Identity Information, Identity Intelligence, and Department of Defense Law Enforcement Criminal Intelligence IV-11

APPENDIX

A Identity Activities Support to Operational Missions A-1
B Assessment Indicators for Identity Activities B-1
C References C-1

GLOSSARY

Abbreviations, Acronyms, and Initialisms GL-1

FIGURE

I-1 Identity Activities Collection, Processing, Exploitation, and Dissemination-Analysis Support Relationship I-5
I-2 Identity Activities Operational Cycle I-8
A-1 Special Operations Forces Exploitation Case Management and Data Transport Architecture A-2
B-1 Example: Objective, Effects, and Indicators for Identity Information and Data (to Include Biometrics, Forensics, and Other Exploitation) B-1
B-2 Example: Objective, Effects, and Indicators for Alien Migrant Interdiction Operations B-3
B-3 Example: Objective, Effects, and Indicators for Base Access, Entry Control Points/Ports of Entry/Maritime Interception/Checkpoints . B-4
B-4 Example: Objective, Effects, and Indicators for Census Operations B-5
B-5 Example: Objective, Effects, and Indicators for Civil-Military Operations B-6
B-6 Example: Objective, Effects, and Indicators for Countering Weapons of Mass Destruction B-6
B-7 Example: Objective, Effects, and Indicators for Chemical, Biological, Radiological, and Nuclear Response Operations B-7
B-8 Example: Objective, Effects, and Indicators for Cordon Operations B-7
B-9 Example: Objective, Effects, and Indicators for Counterdrug Operations B-8
B-10 Example: Objective, Effects, and Indicators for Counter-Improvised Explosive Device Operations B-9
B-11 Example: Objective, Effects, and Indicators for Combating Terrorism Operations B-9
B-12 Example: Objective, Effects, and Indicators for Counterinsurgency Operations B-10
B-13 Example: Objective, Effects, and Indicators for Countering Threat Networks B-10
B-14 Example: Objective, Effects, and Indicators for Cyberspace Operations B-10
B-15 Example: Objective, Effects, and Indicators for Defense Operations B-11
B-16 Example: Objective, Effects, and Indicators for Detainee Operations B-11
B-17 Example: Objective, Effects, and Indicators for Counter-Threat Finance Operations B-12

B-18 Example: Objective, Effects, and Indicators for Foreign Internal Defense Operations B-12
B-19 Example: Objective, Effects, and Indicators for Human Trafficking B-13
B-20 Example: Objective, Effects, and Indicators for Foreign Humanitarian Assistance B-13
B-21 Example: Objective, Effects, and Indicators for Intelligence B-14
B-22 Example: Objective, Effects, and Indicators for Logistics B-15
B-23 Example: Objective, Effects, and Indicators for Military Police Operations B-15
B-24 Example: Objective, Effects, and Indicators for Noncombatant Evacuation Operations B-16
B-25 Example: Objective, Effects, and Indicators for Offense Operations B-16
B-26 Example: Objective, Effects, and Indicators for Peace Operations B-16
B-27 Example Objective, Effects, and Indicators for Personnel Recovery B-16
B-28 Example Objective, Effects, and Indicators for Personnel Screening and Vetting B-17
B-29 Example Objective, Effects, and Indicators for Populace and Resources Control Measures B-17
B-30 Example Objective, Effects, and Indicators for Site Exploitation B-17
B-31 Example Objective, Effects, and Indicators for Stability Activities B-18
B-32 Example Objective, Effects, and Indicators for Support to Targeting B-19

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the application of the Department of Defense identity activities, including related capabilities, functions, and processes, throughout planning, execution, and assessment of maneuver, intelligence, and law enforcement activities in support of military operations.**

- **Outlines the role and placement of identity activities in military operations, and support to military operations, across the competition continuum.**

- **Describes the four identity activity capability sets of biometric collection, storage, and matching technologies; forensic material collection exploitation and preservation processes; document and media exploitation collection, exploitation, and data management capabilities; and identity intelligence or Department of Defense law enforcement criminal intelligence analysis and production.**

- **Lists authorities to conduct identity activities and outlines related legal and policy considerations.**

- **Discusses special considerations for identity activities during multinational operations.**

- **Discusses special considerations for sharing of identity information, identity intelligence, and Department of Defense law enforcement criminal intelligence.**

Overview

The Department of Defense (DOD) employs identity activities for one or more of the following seven primary purposes:

- **Discovery of Threats.** Through the analysis and characterization of encountered persons of interest and their associated groups and networks, identity activities seek to uncover the presence, capabilities, and intent of individual threats, their associates, and networks operating within the operational environment (OE).

- **Risk Assessment**. Identity activities enable the joint force commander (JFC) to more fully understand and evaluate the potential risks presented by individuals

operating within the OE and/or seeking access to military personnel, equipment, or facilities.

- **Targeting.** Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.

- **Attribution.** Identity activities can be used to attribute events, materials, locations, associations, or activities to one or more specific individuals.

- **Support to National Security and Homeland Security.** Outside the United States (in the forward regions and approaches), DOD conducts activities to maintain the freedom to operate in portions of the OE, access information, and conduct operations or campaigns to disrupt and defeat threats before they are able to execute attacks against the US homeland.

- **Support to National Law Enforcement.** National defense or offensive operations include the use of multiple instruments of national power in concert with partner nations (PNs) to achieve both military and national security objectives.

- **Assessment.** Staffs integrate identity activities capabilities to support the continuous assessment of military operations.

Identity Activities

Identity activities are a collection of functions and actions that appropriately recognize and differentiate one person or persona from another person or persona to support decision making. They include the collection of identity attributes and physical materials; their processing and exploitation that informs all-source analytic efforts that lead to the production of identity intelligence (I2) and the development of DOD law enforcement criminal intelligence (CRIMINT) products to inform policy and strategy development, planning, and assessment; enable prosecution; and appropriate action at the point of encounter.

Production of I2 and DOD law enforcement CRIMINT is **directly supported by** the following primary collection, processing, and exploitation capabilities:

- Biometrics.
- Forensics.
- Digital/multimedia forensics.
- Document and media exploitation (DOMEX).

The Relationship Among Intelligence, Maneuver, and DOD Law Enforcement Units

Identity activities provide information on individuals and help establish relationships between individuals, events, devices, and weapons to inform decision making. They discover and contribute information to the all-source intelligence picture on relevant actors and networks, track their movement, help limit target mobility, and enable force protection and civil order. This purpose is supported by a range of specific roles, responsibilities, and actions that are shared, as appropriate, among maneuver, intelligence, and DOD law enforcement organizations to support the JFC or cooperating partner forces.

Identity Activities Support to Military Operations

The Role and Placement of Identity Activities in Military Operations

At the strategic level, identity activities depend upon effective combatant command (CCMD) coordination and synchronization, interagency and PN sharing, multi-component collaboration, and decentralized multidimensional approaches. Strategic partnerships and military engagements yield information and intelligence, thereby informing analytic efforts, producing I2 and/or DOD law enforcement CRIMINT products, and providing actionable decision support to JFCs and national security organizations worldwide.

At the operational level, identity activities use collaborative and decentralized approaches that blend technical capabilities and analytic tradecraft to identify and characterize individuals and networks within the operational area.

At the tactical level, the primary focus of identity activities is identifying persons of interest and determining their disposition at the point of encounter; connecting them to places, people, events, and materials of interest; enhancing force protection measures; enhancing and substantiating targeting activities; and vetting individuals for positions of trust or access.

Support to Military Operations Across the Competition Continuum

Identity activities can be conducted across the competition continuum at all levels of warfare, and throughout an operation or campaign. The JFC integrates and synchronizes identity activities within each phase of an operation regardless of how the phase balance of activities is weighted toward offense, defense, and stability.

Planning Identity Activities

Planning for integrated and synchronized identity activities should address all geographic areas and operations that support global, transregional, and regional operations and campaign plans. This includes the coordination of all instruments of national power, collaboration with the CCMDs to collect and share information using responsible and appropriate mechanisms and safeguards to inform a wide array of missions and activities, and the establishment of technical means and standards to ensure the enterprise can support the timely access, discovery, and use of identity information and analysis.

Planning Considerations

As planning adapts to changing circumstances, it should detail multiple approaches to employ identity activities and enable seamless transition between phases of operations. Commanders conducting operations that include identity activities should ensure that subordinate unit missions are integrated by task and purpose. The commander ensures the concept of operations clearly describes the identity activities scheme of maneuver and expresses how each element can coordinate to accomplish the mission.

Capability Needs Across the Phases of an Operation

Identity activities may be conducted in all phases of an operation to directly enable all subsequent phases and support both the intermediate objectives of the phase as well as the strategic objectives of the operation or a separate campaign. The transition between phases is primarily a function of refocusing efforts toward the evolving objectives. The main challenge for planners is to adeptly plan for timely permissions and authorities to allow deployment and fielding of identity activities capabilities that usually require long lead time.

Additional Planning Considerations

The prevalence and value of information gained by conducting identity activities in today's operations are a function of the exponential increase in technology that has fundamentally changed the way identity information

is collected, processed, exploited, and disseminated. These technologies continue to proliferate and often bridge cultural, geographic, and language barriers. Many technologies enable identity activities to be adaptable in a tailorable and scalable approach to support regionally focused missions, bilateral and multilateral military exercises, and security cooperation activities.

Assessment of Identity Activities

Commanders and their staffs should conduct assessments through a continual process of evaluation and feedback, in which metrics relating to performance and effectiveness of tactics, techniques, and procedures, systems, and networks are collected and used to assess the entire range of identity activity-related capabilities.

Using Identity Activities to Support Operational Assessment

Identity activity indicators help commanders and staffs determine whether they are taking the proper actions to attack enemies and networks operating in their operational area.

Identity Activities Core Capabilities

The four identity activity capability sets employed by the JFC sets include biometric collection; storage, and matching technologies; forensic material collection exploitation, and preservation processes; DOMEX collection, exploitation, and data management capabilities; and I2 or DOD law enforcement CRIMINT analysis and production.

Identity activities core capabilities are present and accessible across multiple US government departments and agencies, as well as multiple multinational elements.

JFCs coordinate and cooperate with multinational partners to execute identity activities. With numerous stakeholders involved in identity activities, unity of effort is critical to success.

Biometrics

Biometrics is an enabling technology that cuts across many activities and operations and is a key enabler of identity activities. Regardless of disguises, aliases, or falsified documents, an individual's biometrics are unique to one individual and can be attributed to one individual and tracked using various devices and repositories that denies anonymity.

Forensics

Forensics is the application of multidisciplinary scientific processes to establish facts that can be used by a JFC to support military operations. Forensic disciplines include DNA, serology, firearms and tool marks, latent prints, questioned documents, forensic chemistry, and trace materials. Forensic capabilities can be used to support intelligence functions, operational activities, force protection, host nation legal support, and other related efforts.

Document and Media Exploitation

DOMEX activities can increase the value of information gained, provide timely and relevant information to commanders, support the intelligence and operational decision-making process throughout the competition continuum, and assist judicial proceedings through application of preservation and chain-of-custody procedures. DOMEX may provide information on the strategies, plans, operations, activities, tactics, weapons, personnel, contacts, finances, and logistics of terrorists, criminal networks, and other threats in the OE.

Identity Intelligence and Criminal Intelligence

I2 and/or CRIMINT driven activities combine the synchronized application of biometrics, forensics, and DOMEX capabilities with intelligence and identity management processes to establish identity, affiliations, associations, and patterns of individual and group behavior to deny anonymity to the enemy or adversary, substantiate attribution, inform targeting activities, and protect PN assets, facilities, and forces.

Special Considerations

Authorities

Pursuant to US and international law, DOD components have authority to collect, process, and exploit identity information, forensic materials, and captured materials. These activities, however, may be subject to limitations, restrictions, or conditions on collection and data use depending on the circumstances (time, place, manner, and purpose) of the activity. Identity activities may be conducted during times of peace or conflict; at home, abroad, or on the high seas. The collection may be obtained through a variety of means and methods, and the identity information may be used for a variety of purposes supporting operations.

Legal and Policy Considerations

Identity activities are likely to involve a myriad of legal and policy considerations. Because of the nature and complexity of the operational legal issues involved, the assigned legal advisor should be consulted early and frequently throughout identity activity planning and execution.

Multinational Operations

US commanders should expect to conduct identity activities as part of a multinational force (MNF) conducting military operations. These operations, which could occur in a formal multinational alliance or a less formal coalition, could span the competition continuum and require coordination with a variety of other interorganizational partners. To effectively employ identity activities, commanders and staffs must be cognizant of differences in partners' laws, doctrine, organization, equipment, terminology, culture, politics, religion, and language, to craft appropriate solutions to achieve unity of effort. Multinational considerations also include international law, agreements, arrangements, and national laws and caveats required to protect the sovereign interests of troop-contributing nations.

Sharing of Identity Information, Identity Intelligence, and Department of Defense Law Enforcement Criminal Intelligence

The amount of identity information or I2 and/or DOD law enforcement CRIMINT products required to be shared varies widely based on the nature of the military operation. In general, combat operations with MNFs require much more robust information and intelligence sharing than humanitarian or peacekeeping operations. The JFC should scale the organization's capability to share identity information, I2, and DOD law enforcement CRIMINT products accordingly.

CONCLUSION

This joint doctrine note addresses how identity capabilities may be coordinated and integrated to create effects across all phases of an operation or campaign. It supplements current joint doctrine and provides context for identity activities across the competition continuum.

Intentionally Blank

CHAPTER I
OVERVIEW

"The United States Government's ability to effectively analyze, evaluate, integrate, correlate, and share [identity attributes and associated information and intelligence] concerning threat actors and their networks, and then use that information to support a broad array of national security missions and activities, is an essential component of our national security strategy."

National Security Presidential Memorandum-7, *Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans*

1. Introduction

This publication guides combatant commanders' (CCDRs'), subordinate joint force commanders' (JFCs'), and component commanders' application of the Department of Defense (DOD) identity activities, including related capabilities, functions, and processes, throughout planning, execution, and assessment of relevant maneuver, intelligence, and law enforcement activities in support of military operations. It describes the specific functions, tasks, and capabilities employed during joint force identity activities, and provides fundamental principles and guidance to plan, employ, and execute identity activities across the various missions and activities, and under the various authorities of joint force components. The information in this publication is not intended to supersede existing joint doctrine that guides military operations and activities, but addresses how a commander should integrate identity activities within planning, execution, and assessment to enhance military operations conducted within a complex operational environment (OE).

a. Commanders and their forces focus on planning and conducting operations, actions, and activities to favorably shape the OE, while also anticipating and preparing to execute contingency responses to crises. Establishing and characterizing the identity of persons of interest, known adversaries, and other relevant actors across the competition continuum is an operational imperative that improves a commander's full understanding of the OE; friendly, threat, and other networks impacting the OE; military interaction with the local population; conduct of military operations; and the long-term security of the United States and its allies.

b. While the capabilities, functions, and processes inherent to identity activities are utilized by multiple United States Government (USG) departments and agencies to support any number of individual applications and uses, DOD employs identity activities for one or more of the following seven primary purposes:

(1) **Discover Threats.** Through the analysis and characterization of encountered persons of interest and their associated groups and networks, identity activities seek to uncover the presence, capabilities, and intent of individual threats, their associates, and networks operating within the OE. Identity activities provide the commander a greater understanding of the threat, their capabilities and capacities, their

facilitation networks and support structures, key personnel, and other relevant actors as well as greater situational awareness. Identity activities provide robust, scalable, and sharable mechanisms to map and monitor human activity, identify network nodes and centers of gravity, and exploit enemy vulnerabilities. Identity activities also provide a means for combat assessment by monitoring the resilience of threat networks after an attack or maneuver (e.g., confirming the capture/kill of a target, confirming a decrease in improvised explosive devices [IEDs] linked to a specific bomb maker or network).

(2) **Risk Assessment.** Identity activities enable the JFC to more fully understand and evaluate the potential risks presented by individuals operating within the OE and/or seeking access to military personnel, equipment, or facilities. The JFC can use identity activities supported by identity intelligence (I2) to rigorously and routinely assess and characterize the level of threat or trust presented by individuals and their networks, to inform follow-on actions, mission planning, screening and vetting, and force protection postures.

(3) **Targeting.** Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. Targeting planners require access to detailed information on targets, supported by the nominating component's analytical reasoning that links the targets with the desired effects. Identity activities provide a persistent supporting capability for JFCs' targeting efforts. Data generated through identity activities about individuals and their associates, as well as their assessed capabilities, capacities, and ideological underpinnings. This data can provide an ample resource to inform the systematic analysis and prioritization of military targets, and subsequently assign and organize appropriate resources for targeting. Identity activities provide a robust capability to identify and track specific individuals across time and space with a high degree of confidence. Moreover, identity activities facilitate a persistent intelligence, surveillance, and reconnaissance (ISR) to understand the actor's habits, behavioral and temporal recurrence, centers of gravity, network components, and areas of exposure or weakness.

(4) **Attribution.** Identity activities can be used to attribute events, materials, locations, associations, or activities to one or more specific individuals. While our peer and near-peer competitors may not be overly eager to enter into armed conflict with the United States, they are more than willing to work to undermine legitimacy, establish and support alternative narratives, and use proxies or other asymmetric means to achieve their strategic objectives. In today's security environment, our ability to quickly, accurately, and defensibly attribute actions, events, or materiel to state or non-state actors has a direct, measurable impact on our ability to respond to the emerging threat and achieve strategic objectives.

(5) **Support to National Security and Homeland Security.** Outside the United States (in the forward regions and approaches), DOD conducts activities to maintain the freedom to operate in portions of the OE, access information, and conduct operations or campaigns to disrupt and defeat threats before they are able to execute attacks against the US homeland. Identity activities inject vital data and information, which can be analyzed and organized into knowledge, facilitating action against threats

and networks (i.e., the discovery of unknowns) and enable corresponding action. Knowledge databases containing information on persons of interest support the national security community, intelligence community (IC), homeland security missions and activities, and partners – ranging from domestic law enforcement and immigration officials to the military, intelligence, and broader security elements of partner nations (PNs).

(6) **Support to National Law Enforcement.** National defense or offensive operations include the use of multiple instruments of national power in concert with PNs to achieve both military and national security objectives. Lethal effects on an enemy may not be authorized, not politically acceptable, or simply not the best course of action (COA). To effectively target these elements, a JFC coordinates with mission partners in a coordinated effort that focuses on, among other things, the use of law enforcement tools, authorities, and reach. The JFC seeks to enable these military-to-law enforcement partnerships through collaborative alignment and conformance to standardize methods and management techniques for collection, processing, exploitation, and information sharing. Among others, key collaborators are the defense attaché and legal advisor(s).

(7) **Assessment.** Staffs integrate identity activities capabilities to support the continuous assessment of military operations. These capabilities assess measures of effectiveness (MOEs), assess measures of performance (MOPs), and support battle damage assessment by providing a scientific means to distinguish one person from another and monitoring individual activity. By processing collected data, identity activities can inform commanders of new vulnerabilities that can be exploited.

c. Identity activities are functions, tasks, processes, and capabilities, planned and conducted in addition to normal military functions. Identity activities should be fully integrated into operational design, joint intelligence preparation of the operational environment (JIPOE), the joint planning process (JPP), operational execution, the joint targeting process, and joint assessments. Identity activities can be conducted throughout all phases of a campaign or operation throughout the OE, and across the competition continuum, to increase the commander's awareness about the OE and enhance the ability to protect the force, persistently target the enemy, and support security and rule of law activities within an operational area.

d. The effective application of identity activities requires a long-term focus and the understanding that, from initial collection and exploitation to any future encounters, each constituent effort is designed to support the broadest array of missions. Without this emphasis, future military operations could be undermined, degrading our ability to achieve mission objectives. Similarly, broader national security activities related to defeating terrorist networks, protecting our borders, and dismantling criminal networks will be adversely affected.

e. Identity activities are neither a mission nor an application (like joint close air support). They do not formally standardize, direct, or control component usage or programmatics, nor do they convey any new or additional roles or authorities. They are simply an organizing construct established to guide planning, application, and

management of related capabilities by a JFC to support missions or operations that leverage or require identity information and analytic judgment to support decision making.

f. For this reason, DOD components may or may not refer to their existing supporting programs as identity activities, while still providing capabilities that execute the function, tasks, and processes that comprise the identity activities construct. Defense intelligence components like the Army Deputy Chief of Staff for Intelligence or the Marine Corps Intelligence Activity refer to their programs as I2. The Defense Intelligence Agency (DIA) describes its biometric, forensic, and document and media collection and exploitation capabilities as measurement and signature intelligence and document and media exploitation (DOMEX), respectively. United States Special Operations Command (USSOCOM) describes its program of record as sensitive site exploitation and its use as I2 operations within USSOCOM policy directives. The United States Marine Corps describes its program and strategy as identity operations, while the United States Navy and United States Army Provost Marshal General call their programs identity activities. Similarly, program initiatives at the combatant commands (CCMDs) vary between identity activities and I2, depending on which CCMD staff organization has primary management responsibility (e.g., operations directorate of a joint staff [J-3] or intelligence directorate of a joint staff [J-2]). Regardless of a component organization's chosen terminology, the identity activities construct and its characteristic considerations described below provide a common and repeatable framework for planning, execution, and assessment. In each program instance, there are more similarities in function and design than there are differences. The differences typically lie in the individual authorities for collection and use of identity information, the differing levels of fidelity of exploitation capabilities, and the considerations taken for using collectable exploitable materials for intelligence uses versus or concurrently being used for evidence.

2. Identity Activities

Identity activities are a collection of functions and actions that appropriately recognize and differentiate one person or persona from another person or persona to support decision making. They include the collection of identity attributes and physical materials; their processing and exploitation that informs all-source analytic efforts that lead to the production of I2 as well as the development of DOD law enforcement criminal intelligence (CRIMINT) products to inform policy and strategy development, planning, and assessment; enable prosecution; and appropriate action at the point of encounter. Summarized, identity activities may result in all-source analysis and production enabled by conventional forces (CF) and special operations forces (SOF) collection, processing, exploitation, and data dissemination capabilities to support the commander's decision-making process. Information and intelligence obtained via such activities as biometrics-enabled intelligence (BEI), forensic-enabled intelligence (FEI), and DOMEX can be used to help identify people and groups. This relationship is depicted in Figure I-1.

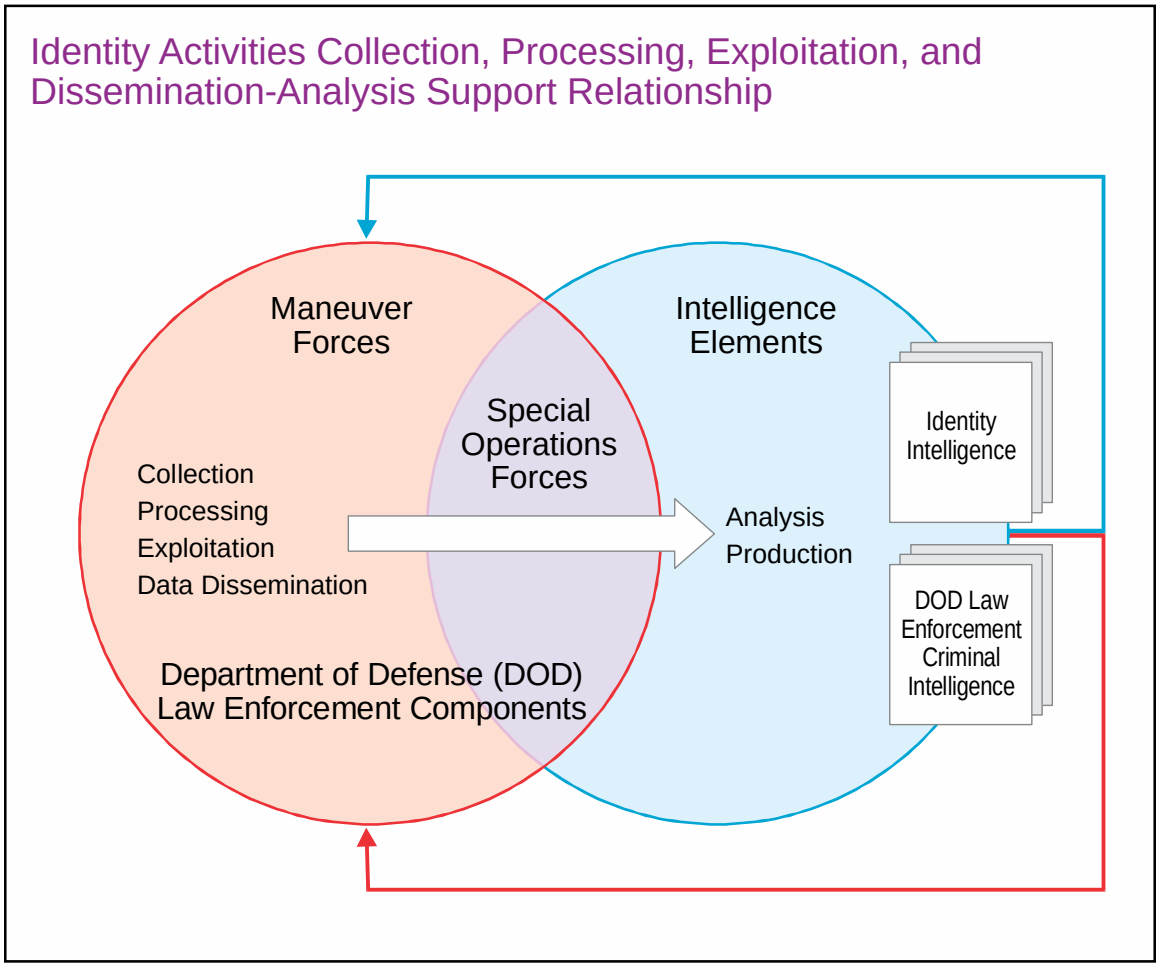


Figure I-1. Identity Activities Collection, Processing, Exploitation, and Dissemination-Analysis Support Relationship

a. The use of identity to inform decision makers is commonplace across the joint force. Accordingly, the functions, missions, collection of actions, and individual actions that comprise identity activities can be conducted jointly and independently by maneuver, intelligence, and/or DOD law enforcement units across their individual missions and authorities. Given the unique attributes and authorities of each functional community and their varying degrees of relevance for any given mission set and phase of operation, identity activities do not establish a hierarchy of users, functions, outcomes, force providers, or mission priorities. Instead, they enable the JFC to make optimal use of both identity information and available identity-related capabilities to support military operations and activities, while simultaneously enabling strategic efforts to achieve broader national security objectives.

b. Foundationally, identity activities are executed to support decision making at the tactical, operational, and strategic levels. Such decision support is most routinely provided through the production of I2 and/or DOD law enforcement CRIMINT products.

(1) **I2** is the intelligence resulting from the processing and characterization of identity attributes concerning individuals, groups, networks, or populations of interest. I2 fuses identity attributes (e.g., biographical, biological, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes, collected across multiple activities, sources, and methods, to identify, assess, and characterize threats and networks, their capabilities and capacity, centers of gravity, objectives, intent, and potential COAs.

(2) **DOD law enforcement CRIMINT** products are the result of the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities in an effort to anticipate, prevent, or monitor criminal activity. DOD law enforcement CRIMINT utilizes information gathered from law enforcement sources, in a manner consistent with applicable law, to provide tactical and strategic criminal intelligence on the existence, identities, and capabilities of criminal suspects and organizations. DOD law enforcement CRIMINT analysis is conducted under circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity that has a connection to DOD.

For more information, see Department of Defense Instruction (DODI) 5525.18, Law Enforcement Criminal Intelligence (CRIMINT) in DOD.

c. Production of I2 and DOD law enforcement CRIMINT is **directly supported by** the following primary collection, processing, and exploitation capabilities:

(1) **Biometrics.** Biometric identification is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. This includes the use of collection, processing, storage, matching, and sharing of biometric data and associated biographic and contextual information from enemy combatants, adversaries, and unknown local populations to support military operations and activities.

(2) **Forensics.** Forensics is the application of multidisciplinary scientific processes to establish facts. This includes the collection, processing, preservation, storage, exploitation, and sharing of collected exploitable materials obtained through the course of military operations and activities organized to achieve a specific objective in a foreign country.

(3) **DOMEX.** DOMEX is the processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under the USG's physical control. This includes the collection, processing, translation, exploitation, analysis, and dissemination of documents and media obtained through the course of military operations and activities organized to achieve a specific objective in a foreign country. Captured documents and media, when processed and exploited, may provide valuable information such as adversary plans, intentions, locations, capabilities, and status. The category of "captured documents and media" includes all media capable of storing fixed information to include computer storage material. DOMEX is not solely

conducted by intelligence personnel and is also conducted by law enforcement and maneuver forces. Digital/multimedia forensics is the application of computer science and investigative procedures in the examination of digital and/or multimedia material.

For more information on how these capabilities directly support identity activities, see Chapter III, "Identity Activities Core Capabilities."

d. These capabilities, and the functions and tasks they support, can be executed individually by either intelligence and DOD law enforcement units operating under their individual mission authorities, or by conventional and special operations maneuver units executing an operation or campaign either individually or in concert.

e. Identity activities leverage a nonlinear and recurrent cycle of collection, processing, exploitation, and data dissemination and all-source analysis and production capabilities to support decision making and to enable prosecution. They require unity of action between collection, processing, and exploitation and all-source analysis and production to create actionable information. Each step of the cycle can result in actionable information to inform the commander's decision-making process, as well as future planning. The tasks within the identity activities operational cycle are conducted continuously as part of tactical operations executed across the OE. This cycle is depicted in Figure I-2.

f. Due to the sensitivities of personal information, variances in social or cultural norms, and international concerns about privacy and civil liberties, the joint force will need to employ appropriate safeguards to protect identity information and I2 products from inappropriate access or use.

g. To employ identity activities, joint force components and organizations conduct six interrelated tasks to provide commanders with relevant assessments and estimates to inform decisions. These tasks integrate the roles of the planner, operator, examiner, analyst, and commander into a single cycle to ensure robust support to military operations. The six tasks are:

(1) **Plan and Direct.** Planning and direction functions include, but are not limited to the identification and prioritization of identity-related information collection requirements; the development of a concept of operations (CONOPS) and architectures required to support the commander's mission; tasking subordinate maneuver, intelligence, and/or law enforcement elements for the collection of identity information and, where appropriate, the production of I2 or DOD law enforcement CRIMINT; submitting requests for additional collection, exploitation, or analytic capabilities to higher headquarters; and submitting requests for collection, exploitation, or all-source production support to external supporting entities (e.g., multinational partners, host nation [HN], interagency elements). Identity activities planning and direction occurs continuously as part of the command's adaptive planning effort. Support to planning enables prioritization of identity activity capabilities across all ongoing operations and simultaneous planning efforts and products, such as JIPOE, informs the development and prioritization of capacity, and enhances readiness to respond to potential crises. Through

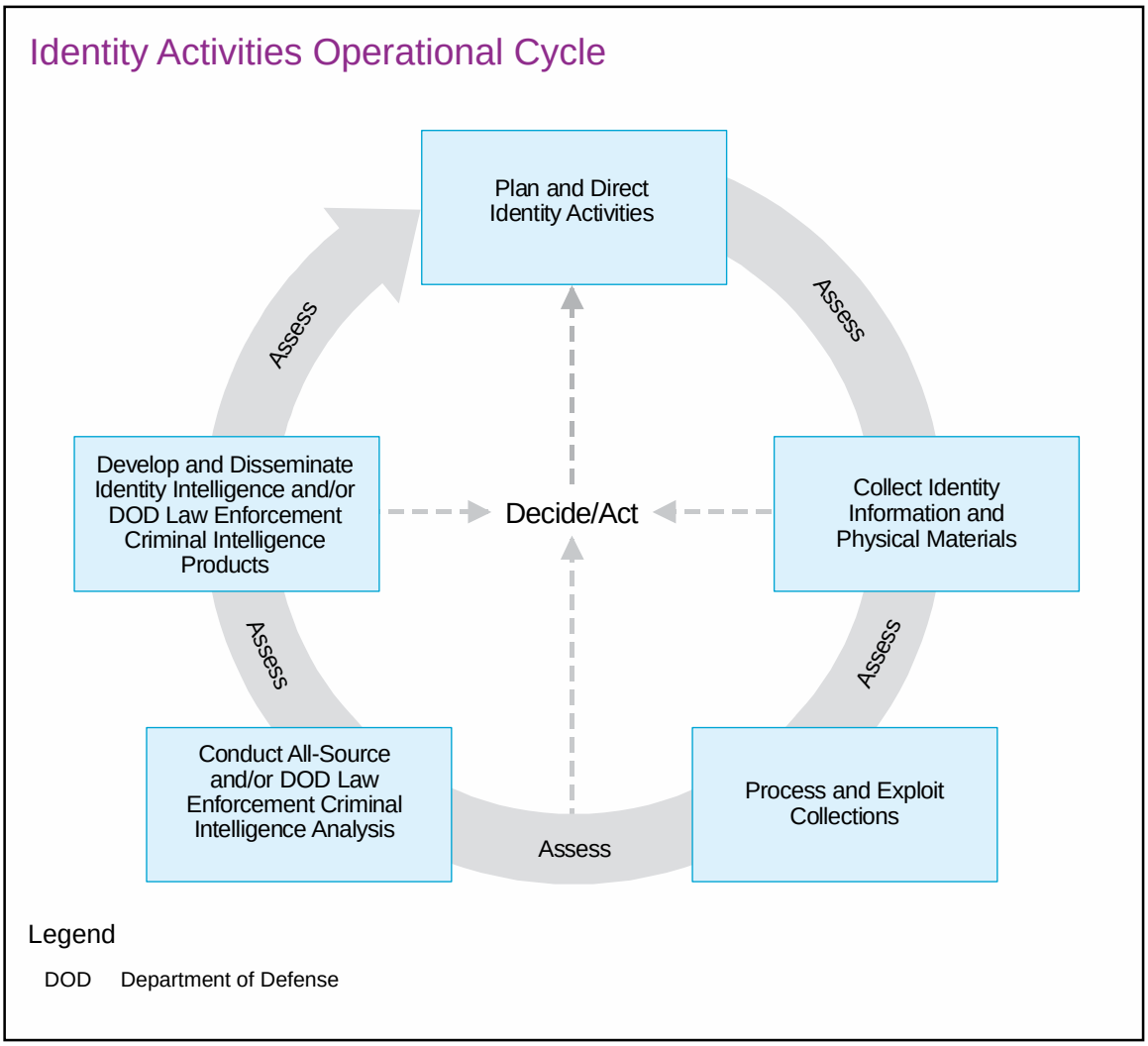


Figure I-2. Identity Activities Operational Cycle

these efforts, planners determine the personnel, equipment, and information sharing and intelligence architecture essential for identity activity support to joint operations.

(2) **Collect Identity Information and Materials.** Collection includes those activities related to the acquisition of identity attributes (i.e., biologic, biographic, behavioral, and reputational data), forensic materials, and documents and electronic media of interest. Collection can be conducted by military forces, DOD law enforcement agencies, USG interagency partners, and foreign partners. While some identity information (i.e., attributes contained on an identity credential) can be used immediately at the point of collection, most collected data and materials are sent to authoritative data repositories or local, regional, or reachback facilities or laboratories (including interagency partners) for appropriate processing, exploitation, and long-term storage.

(3) **Process and Exploit Collections.** During processing and exploitation, raw collected identity data and physical materials can be examined and analyzed by

automated systems and/or trained personnel to determine their information value, correlate data to previously collected data, and report findings to command and I2 analysts. Processing and exploitation include data normalization, biometric matching, forensic analysis, technical (i.e., electronic and mechanical) analysis, and, in some cases, document and media translation and content analysis as well as reporting the results of these actions to appropriate intelligence and/or law enforcement production elements. Processing and exploitation may be federated or performed by the same element that collected the data.

(4) **Conduct All-Source Analysis.** Identity activities can provide valuable information to the command, IC, and law enforcement community. I2 can expose the JFC to a broader understanding of individual threats. DOD law enforcement CRIMINT, in a similar manner, can support the rule of law. I2 utilizes enabling intelligence analysis activities, like BEI, FEI, and DOMEX to discover the existence of unknown potential threats; associate individuals to other persons, places, events, or materials; analyze patterns of life; and characterize their level of potential threat to US interests.

(5) **Develop and Disseminate I2 and/or DOD Law Enforcement CRIMINT Products.** I2 and DOD law enforcement CRIMINT production exists in many forms. They may be oral presentations, printed publications, or electronic media. The means are determined by the needs of the user and the implications and criticality of the intelligence. Rather than being the end of a process, I2 and/or DOD law enforcement CRIMINT production is a continuous dialogue between the user and the producer. Units and organizations at every echelon produce I2 for joint operations. However, reachback elements like joint intelligence operations centers (JIOCs), Service intelligence centers, and CCMD-assigned intelligence brigades typically form the backbone of any operational I2 production support. DOD law enforcement agencies and units create DOD law enforcement CRIMINT products, which may be provided as supporting information to the JFC.

(6) **Conduct Assessments of Identity Activities.** Commanders and their staffs conduct assessments of identity activities to determine whether they are generating the desired products to support military operations. Identity activities require a greater application of operational art due to the complexity of the human dimension of the OE. Likewise, identity activities' assessments require staffs to conduct analysis more intuitively, considering both anecdotal and circumstantial information. Assessments over time that show trends are much more valuable for identity activity planning and operational support than a single snapshot covering a short time frame. Tactical unit reporting, such as patrol debriefs and unit after-action reports, may provide the most valuable information on assessing the impact of identity activities, particularly when correlated across an OE.

3. The Relationship Among Intelligence, Maneuver, and DOD Law Enforcement Units

Identity activities provide information on individuals and help establish relationships between individuals, events, devices and weapons to inform decision making. They

discover and contribute information to the all-source intelligence picture on relevant actors and networks, track their movement, help limit target mobility, and enable force protection and civil order. This purpose is supported by a range of specific roles, responsibilities, and actions that are shared, as appropriate, among maneuver, intelligence, and DOD law enforcement organizations to support the JFC or cooperating partner forces.

a. Identity activities functions and actions are supported by three primary types of organizations:

(1) **Maneuver Units.** Deployed maneuver units provide multiple Service collection, processing, and exploitation capabilities to support military operations. These activities often provide the basis for all-source intelligence analysis supporting the production of I2 to meet the commander's information requirements. These products, in turn, inform, enable, and enhance continuous operational activities planned and executed by maneuver units to achieve the commander's military objectives.

(2) **Intelligence Elements.** Intelligence elements can conduct collection, processing, and exploitation activities under their own individual authorities in support of the JFC without the capabilities of maneuver or DOD law enforcement units. Their primary contributions to the JFC requirements, however, are analysis and production capabilities, reachback support, specialized technical exploitation capabilities, and foreign disclosure.

(3) DOD **Law Enforcement Units.** Similarly, DOD police; Military Department investigative services (e.g., Naval Criminal Intelligence Service, Army Criminal Investigation Command); Army and Marine Corps military police, Air Force security forces, and Navy master at arms; and other law enforcement capabilities (e.g., Federal Bureau of Investigation [FBI], United States Customs, United States Coast Guard) can conduct collection, processing, and exploitation activities under their own individual authorities in support of the JFC without requiring the capabilities of maneuver or intelligence units. They may also produce DOD law enforcement CRIMINT to support military criminal investigations and military prosecution activities.

b. The question of which organization holds primacy over identity activities operational arrangements, plans, or actions for the command depends on what mission or activity is being supported, the time-sensitivity of the desired effects, and the primary focus of the JFC's military objectives. For instance, early in an operation, a JFC may prioritize and align to identity activities to better understand and monitor the operational area, answer the critical intelligence requirements, and develop and execute a robust target list. During combat, the JFC may concentrate identity activities in support of maneuver operations, with support from intelligence organizations to inform mission planning and assessment, and support from DOD law enforcement forces to manage detainees, internally displaced persons, and force protection activities. This balance may shift again during stabilization, when the JFC requires the collaborative efforts of all three communities to create the desired effects under a designated task force (TF). Whereas in the enable civil authority phase, the JFC may choose to completely shift the

identity activities focus to supporting HN rule of law, and the identification, tracking, detention, and criminal prosecution of individuals working to attack or obstruct the local government or terrorize the local population.

c. Ultimately, the commander arranges, aligns, and mobilizes forces to conduct the mission to achieve the objective. However, it remains important for military planners to keenly understand that no single component or community can provide fully optimized or even completely adequate support to military operations across the competition continuum. Each force provider, to include USSOCOM, can offer forces specifically trained and equipped to execute identity activities functions and tasks that support and enable their specific mission focus and specialty (e.g., USSOCOM employs special operations-unique capabilities, Marines deploy with expeditionary capabilities optimized for traditional Marine Corps missions, the Army's forensics exploitation laboratories (FXLs) provide multidisciplinary capabilities across the forensics disciplines, DIA provides highly specialized collection and exploitation capabilities in support of strategic intelligence priorities). Just as a CCDR relies on a ready and able joint force to execute the complexity of military requirements, multiple force providers will likely be required to meet a JFC's identity activities capability and capacity requirements resident throughout an operation or campaign.

Intentionally Blank

CHAPTER II
IDENTITY ACTIVITIES SUPPORT TO MILITARY OPERATIONS

1. The Role and Placement of Identity Activities in Military Operations

a. Identity activities enable safe and effective operations by providing essential information on the relevant actors and networks to inform planning, execution, and assessment throughout an operation or campaign. Identity activities provide a correlating mechanism to link identity information to other collected information to create an extensive knowledge base of the enemy, adversary, friendly, and neutral variables that characterize the OE. This knowledge base increases the overall understanding of the physical, cultural, and social environment in which the joint force operates and helps to create desired effects across the OE. Exploitation of this body of information more effectively influences the OE, enhancing the ability to control the population, influence key actors, and diminish the enemy's freedom of maneuver.

b. At the strategic level, identity activities depend upon effective CCMD coordination and synchronization, interagency and PN sharing, multi-component collaboration, and decentralized multidimensional approaches. Strategic partnerships and military engagements yield information and intelligence, thereby informing analytic efforts, producing I2 and/or DOD law enforcement CRIMINT products, and providing actionable decision support to JFCs and other national security organizations worldwide. JFCs and their staff must have a thorough understanding of the legal, policy, and architectural frameworks to effectively conduct identity activities across the competition continuum. Identity activity requirements should be integrated in CCMD policies, guidance, orders, and instructions, and should be synchronized and integrated throughout staff planning processes. Pre-mission and contingency planning should include study and integration of strategic and operational-level lessons and arrangement of joint, interagency, and multinational sharing arrangements and Service-level agreements.

c. At the operational level, identity activities use collaborative and decentralized approaches that blend technical capabilities and analytic tradecraft to identify and characterize individuals and networks within the operational area. Specialized collection tools and exploitation processes, combined with all-source intelligence analysis of the collected data, enable commanders to better understand assigned operational area by identifying the actors within it. Operational level echelons employ identity activities and capabilities throughout the OE to support many of their core mission sets. JFCs coordinate and synchronize identity activities at the operational level to ensure friendly force plans and operations are complementary. For example, in Operation ENDURING FREEDOM, the initial organization of deployed forensic exploitation assets created redundancy and inefficiency between counter-improvised explosive device (C-IED)-focused labs and other deployed assets. Only after formal joint force staff structures were put in place and operational control (OPCON) of the resources realigned, was the full efficacy of the capability demonstrated through significantly increased operational support.

d. At the tactical level, the primary focus of identity activities is identifying persons of interest and determining their disposition at the point of encounter; connecting them to places, people, events, and materials of interest; enhancing force protection measures; enhancing and substantiating targeting activities; and vetting individuals for positions of trust or access. Effective use of these activities helps to restrict enemy or adversary mobility, identify threats, monitor or track persons of interest, and manage detainees and displaced persons. Identity activities strip away anonymity and help to counter espionage, sabotage, subversion, insurgency, terrorism, and crime. They enable civil control; separation of warring factions; HN rule of law activities; evaluation of persons for amnesty, reintegration, and reconciliation programs; investigation of crimes against humanity; and transition to civil authority. Identity activities help to shape the OE, deter threats and networks, reestablish safe and secure environments, provide more effective humanitarian relief, and develop or strengthen the legitimacy of HNs, while enhancing and reinforcing PN and HN efforts.

e. Identity activities may support all joint functions across the competition continuum. The broad nature of identity activities can provide useful information to support operational art and operational design during planning. The ways in which identity activities are conducted are often just as important as access to the adequate means to conduct them. JFCs can choose multiple operational approaches to employ identity activities throughout an operation to support achievement of military objectives. Each approach has advantages and drawbacks but all may be restricted in their implementation if adequate pre-mission planning does not occur.

2. Support to Military Operations Across the Competition Continuum

Military operations vary in scope, purpose, and conflict intensity. Military operations and integrated campaigns conducted within the competition continuum require the skillful combination of military engagement, security cooperation, and deterrence activities to crisis response and limited contingency operations and, if necessary, to large-scale combat operations, which take place across the competition continuum. Identity activities can be conducted across the competition continuum at all levels of warfare, and throughout an operation or campaign. The JFC integrates and synchronizes identity activities within each phase of an operation regardless of how the phase balance of activities is weighted toward offense, defense, and stability.

a. JFCs use identity activities in a wide variety of environments as part of a cohesive plan to support the combatant command campaign plan (CCP). Identity activities support scalable, distributed operations performed by CF, SOF, or supporting interagency elements with adequate training and standardized equipment. Identity activities may support building PN capacity, deterring local or regional threats and networks, and enabling crisis response operations or limited contingencies to countering terrorist incidents and supporting large-scale combat operations and campaigns that protect or advance national security interests.

b. JFCs execute identity activities to enhance their ability to protect personnel and property; identify threats; identify personnel who are authorized access to critical

infrastructure, key assets, and cultural properties; manage populations and resources; and screen select persons for positions of trust. Identity activities enable JFCs to better understand the population and OE, protect relevant populations, and promote a PN's legitimacy and influence over a population. These activities enhance scalable sustainable approaches to preventing, deterring, disrupting, or defeating irregular threats and are important to deny irregular threats the resources, cover and concealment, and maneuver offered by local populations.

(1) **Military Engagement, Security Cooperation, and Deterrence Activities.** Military engagement, security cooperation, and deterrence are ongoing specialized activities that establish, shape, maintain, and refine relations with other nations at all levels of conflict. The primary purpose of these activities, which may include identity activities, is to enable the commander to build foreign partner capabilities that deter threats and networks and shape the OE to a desired set of conditions that facilitate stability activities and future operations. Shaping activities include development of PN and friendly military capabilities and capacity, identity information exchange and I2 and/or DOD law enforcement CRIMINT sharing, interagency coordination, and other efforts to ensure access to and stability of critical regions around the globe.

(a) Identity activities support military engagement activities conducted by DOD components and their subordinate units (e.g., Office of the Secretary of Defense [OSD], Naval Criminal Investigative Service [NCIS], US Army Criminal Investigation Command, US Air Force Office of Special Investigations, SOF). CCDRs conduct routine military engagements to build trust and confidence, share information, coordinate mutual activities, maintain influence, build defense relationships, and develop allied and friendly military capabilities for self-defense and multinational operations. DOD components conduct military engagement with nations' military or civilian security forces and authorities. During military engagement, the United States and its partners may establish supportive partnership agreements on conducting identity activities or handling identity information between US forces and the PNs' armed forces.

(b) Security cooperation is DOD interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a PN.

(c) Deterrence of an enemy who uses terrorism, illicit means, or asymmetric methods to achieve its objectives is a difficult task. Identity activities support to deterrence reduces threats and network activity by presenting a credible threat of identification, tracking, and specific counteraction that would deny the success of an organization's use of terrorism, criminal enterprise, and/or guerilla tactics or degrade its legitimacy or influence over a population. Identity activities enable deterrence by delivering relevant identity information on key persons and materials and their associations to a certain time, place, activity, event, or person known to the JFC. This information can be used to deter malicious activity or deny key individuals' mobility or access to resources, track movement, identify contacts and associates, and reveal their

actions. Deterrence in one region may force threats to temporarily move to another, which may deter or disrupt the organization's activities for a period of time.

(2) **Crisis Response and Contingency Operations**

(a) **Crisis Response.** The President and the Secretary of Defense (SecDef) can respond to imminent threats or actual acts of terrorism by executing Chairman of the Joint Chiefs of Staff's or CCDR's contingency plans. Identity activities can provide immediate enhancement to force protection activities, persistent targeting of known threats, and support a variety of offensive, defensive, or stabilization tasks or activities.

(b) **Contingency Operations.** Identity activities during contingencies may include identification of insurgents, terrorists, or criminals and efforts to gain insights into threat and facilitation networks that pose an imminent threat to a US mission abroad. After threats and their organizations are identified and located, US forces may use I2 products to inform and enable strikes or raids to neutralize or reduce the threats, as well as other operations as directed by SecDef or a CCDR.

(3) **Large-Scale Combat Operations.** The JFC may conduct identity activities in support of all phases of operations to disrupt enemies' and adversaries' use of asymmetric tactics and enable a more comprehensive understanding of the OE. Identity activities support the restriction of enemy and adversary mobility within and outside the assigned operational area through the use of biometric-enabled control measures (such as facial recognition at airports, train stations, border control points and ports). Identity activities can identify key personnel and provide means of physical access control to key infrastructure such as financial, healthcare facilities, military bases, and government buildings. Identity activities enable monitoring or tracking of persons of interest and facilitate the vetting of individuals for positions of trust. Identity activities in support of major operations and campaigns should be sustained, synchronized, and integrated across multiple operational areas, and designed to support both current operations and potential follow-on operational phases.

c. **Security Cooperation.** Identity activity support to security cooperation may include:

(1) **Security Sector Assistance (SSA).** SSA equips, trains, and develops capabilities and capacities in foreign military and security forces. A CCP may include activities to provide identity activity-related security assistance to a nation's military and, when authorized, civilian security forces, and may be combined with similar security assistance to neighboring nations to develop regional identity activity capabilities to address cross-border threats and act in a coordinated effort. SSA related to identity activities must be well coordinated with the Department of State (DOS) and interagency partners to ensure unity of effort and synchronization in our military engagements with PNs.

For more information, see Joint Publication (JP) 3-20, Security Cooperation.

(2) **Foreign Internal Defense (FID).** US military support to FID focuses on operational assistance to HN personnel and collaborative planning with interorganizational and HN authorities to anticipate, preclude, and counter threats. FID supports HN internal defense and development programs. US FID programs may use identity activities to help a nation defeat an organized movement attempting to overthrow its lawful government or address other threats to the internal stability of an HN, such as civil disorder, illicit drug trafficking, and terrorism.

For more information, see JP 3-22, Foreign Internal Defense.

(3) **Security Force Assistance (SFA).** SFA may provide identity activity training and equipment to foreign security forces; access to DOD processing and exploitation capabilities; and sharing of relevant identity information, I2, and DOD law enforcement CRIMINT. Supported by appropriate policy and legal frameworks, building capacity and capability is a long-term continuing process enhancing the HN's human, technological, organizational, institutional, and resource capabilities. These capabilities and associated results should be self-sustaining for the HN. Designing capacity and capability building initiatives for identity activities requires an understanding of what identity management processes the HN has in place and the sustainability requirements for any new or additional capabilities introduced. All identity activity initiatives must consider the potential for misuse; the political, social, and cultural sensitivities of the targeted population; and public perception. The primary role of identity activities in SFA is to develop identity activity capabilities and capacity within the HN's security forces. However, joint forces may also have a role to support efforts led by other USG departments and agencies to enhance the partner's identity activity abilities supporting broader elements of governance, economic development, essential services, rule of law, and other critical government functions.

For more information, see JP 3-20, Security Cooperation.

3. Planning Identity Activities

a. Planning involves an analysis of the organizational structure, required resources, and supporting forces available to perform the task, identification of operational limitations, and an assessment of risk. Planning for integrated and synchronized identity activities should address all geographic areas and operations that support global, transregional, and regional operations and campaign plans. This includes the coordination of all instruments of national power, collaboration with the CCMDs to collect and share information using responsible and appropriate mechanisms and safeguards to inform a wide array of missions and activities, and the establishment of technical means and standards to ensure the enterprise can support the timely access, discovery, and use of identity information and analysis. For planners to successfully integrate and synchronize identity activities, commanders provide guidance to identify, characterize, and target threats and elements of the threat network, effectively monitoring and assessing threats and network activities, training the force in identity activities, and transferring equipment and capabilities to participating multinational force (MNF) partners and the HN to support operations. Planning for identity activities should be an

integral part of the overall CCP and subordinate plans. The actual planning and conduct of theater identity activities will depend on the security agreements with HNs, capabilities of the HN forces, the HN's policies, time phasing of available US capabilities, and quality of the JIPOE assessment. The identity activities requirements will be established by the JFC. For identity activities to be effective, they must be viewed in the context of the larger whole-of-government operation or campaign plan and integrated across all staff sections and functional areas.

(1) Identity activities require a clear understanding of the personnel available, their level of training, and in what capacity they can support identity activity tasks. A maneuver unit will have different tasks, training, and capabilities than a weapons intelligence team with specialized search techniques and forensic equipment. Additionally, available equipment (e.g., biometric collection devices, presumptive testing kits, expeditionary exploitation equipment) influences COA development. Commanders consider the time available for identity activity planning and the time sensitivity of the collected information, collected exploitable material, and personnel detained on site. The availability of supporting agencies that provide enabling capabilities, such as information processing, technical analysis, forensic collection and exploitation, and render safe capabilities, also influences identity activity planning and COA development. Commanders, coordinating staffs, and liaison officers identify capabilities and limitations of the assets associated with their respective area of expertise.

(2) Identity activities must be planned and executed within the physical and diplomatic constraints of the operation. Examples of constraints for identity activities planning include, but are not limited to, rules of engagement (ROE), search restrictions relating to gender, and rules for the use of force (RUF). Constraints affect COA development of both the parent unit and subordinate elements. Constraints are considered as tasks and included in the coordinating instructions in operation orders to account for the impact on identity activity planning and execution.

(3) Leaders at all echelons conduct risk assessments before each tactical collection or exploitation activity. The purpose of risk management is to implement controls that remove hazards or reduce the residual risk to an acceptable level. Commanders and leaders at all levels need to know the hazards associated with identity activities. There are instances where the collection, handling, and processing of information and collected exploitable material is of paramount importance and can potentially place personnel at risk. Commanders and leaders minimize risk by establishing mitigation measures and safety guidelines before conducting tactical collection and/or exploitation.

b. The commander's critical information requirements (CCIRs) and other information requirements help focus the staff's planning efforts. The CCIRs can be time-sensitive, especially when related to targeting or countering threat networks. The CCIRs are specific enough to assist the staff in understanding what personnel and equipment are required for identity activity support to a specific action. Staffs recommend intelligence requirements for designation as priority intelligence requirements (PIRs) to gain additional information about the threat and the OE. Lessons learned from recent

operations show that some missions sets require civil information and sociocultural analysis as a PIR.

c. Whether conducting identity activities is the primary mission or planned as a subsequent or secondary task, identity activities COA development follows the same considerations of any planning effort. When developing COAs, the commander and staff task-organize to perform specific identity activity tasks. Enablers are sometimes required to augment the collection and/or exploitation element to provide specialized capabilities to the executing unit(s). When establishing the support relationships, commanders consider the supporting distance and prioritization of use for specialized supporting agencies.

(1) Identity activities should be addressed at the appropriate level in each COA and describe who will conduct the identity activity, what type of identity activity/function will occur, when it will begin, where it will occur, why the identity activity is required (purpose), and how it will occur (method of employment). Commanders should seek to integrate both multifunction and specialized identity activity collection elements within each COA to maximize coverage and availability of forces to meet mission objectives. Whenever possible and appropriate, mission planners should design for and enable PN forces to lead identity activity collection efforts.

(2) During COA analysis, planners should take into account sensitivities and potential reactions among the target population. A staff judge advocate (SJA) review might be necessary to determine the permissibility of collecting identity activity information and data among the target population, in accordance with existing US and HN laws and policies and agreements with the HN.

(3) Staffs should consider how identity activity can be effectively compared between COAs and how those comparisons can illuminate risk. Since identity activities can be disproportionately affected by sociocultural dynamics, HN and PN legal limitations, and technical constraints, consideration should be given to the advantages and disadvantages of including or eliminating identity activities, who should conduct identity activities, what types of collection and exploitation should be included, and the political and cultural risks of conducting identity activities within each COA. Upon selection of the preferred COA, JFCs should ensure relevant interagency partners, country teams, and DOD components are notified and/or coordinated with on the identity activities aspects of the COA, as appropriate or required.

d. During CONOPS development, the commander should determine, and express in sufficient detail to identify specified and/or implied tasks, the best arrangement of simultaneous and sequential identity activities required to accomplish the assigned mission.

e. Identity information and data collection and exploitation should be included in every operation order to the extent appropriate for the operation. Identity activity considerations should be discussed in any applicable place in a plan or order but should be specifically considered for the following annexes and appendices: annex B

(Intelligence); annex C (Operations); annex E (Personnel); annex G (Civil-Military Operations [CMO]); appendix 14 (Force Protection) to annex C (Operations); and annex W (Operational Contract Support [OCS]).

4. Planning Considerations

Plans should incorporate those identity activities that best contribute to mission accomplishment. As planning adapts to changing circumstances, it should detail multiple approaches to employ identity activities and enable seamless transition between phases of operations. Commanders conducting operations that include identity activities should ensure that subordinate unit missions are integrated by task and purpose. The commander ensures the CONOPS clearly describes the identity activities scheme of maneuver and expresses how each element can coordinate to accomplish the mission. Commanders ensure their forces are properly trained and that all echelons of leadership have an understanding of how identity activities contribute to and further enable the achievement of mission objectives.

a. To properly apply the suitable level of identity activities, planning should provide a broad framework of the facts and assumptions about the OE. It should provide a perspective on who will conduct certain actions, what resources are available, and how the plan is to be implemented. The plan should also incorporate the transition of identity activities from phase to phase and to account for the consolidation of gains and changes in the characterization of the OE throughout the operation or campaign.

b. CCDRs and their staffs incorporate appropriate identity activities during the planning, execution, and assessment of large-scale combat and contingency operations as well as security cooperation activities and stability activities. The key planning considerations are:

(1) Plan for the integration and interoperability of identity activities support to operations, security cooperation, and other activities in support of the CCPs.

(2) Establish interorganizational cooperation involving identity activities early in the planning process.

(3) Coordinate with assigned legal advisors frequently to ensure compliance with US laws and policies, international agreements, treaties, and PN laws regarding the collection, processing, storage, and sharing of identity-related information.

(4) Ensure that potential threats, known threats, and their supporters are immediately nominated to the DOD biometric-enabled watchlist (BEWL), the authoritative watchlist for the command, and when they meet the threshold for the National Known or Suspected Terrorist Watch List, to the National Counterterrorism Center through DIA.

(5) Establish necessary joint, interagency, and multinational sharing arrangements and Service level agreements to support component collection efforts.

(6) Establish theater-specific operation policies, procedures, and CONOPS, where appropriate.

c. Commanders should pay particular attention to their environment, influence, and limitations as the ability to collect and exploit identity data can vary greatly based on several key factors:

(1) **Possible Limitations on Identity Activities.** Identity activities may be limited or restricted completely for some situations. Capabilities should be employed to the extent conditions allow and commanders should not exceed their collection and exploitation authorities. Depending on the mission, certain identity data may be collected via different means or elements of identity activities; I2 may not be required, permissible or applicable. For example, one theater may require voluntary participation for identity enrollment, where in another area of responsibility (AOR) compulsory enrollment may be permissible based on the approved ROE.

(2) **Need for Interorganizational Sharing.** Interorganizational sharing of appropriate identity information will be critical to protecting the homeland and interests abroad, deterring and preventing conflict, shaping regional stability, and assuring allies and PNs of our commitment to shared security. To foster this sharing, identity activities should prevent the classification of raw, unexploited materials, and extracted data realizing that even the designation of "For Official Use Only" or other handling restrictions, can also hinder sharing. The challenge is to find a suitable balance between the growing need to share relevant information and the need to enforce applicable policies to protect certain information.

(a) Increased interagency cooperation is vital in conducting crisis response and contingency operations that bring all instruments of national power to bear. Establishing interagency coordination reduces duplication and maximizes the use of limited resources. CCDRs should develop plans and policies that delineate the roles and responsibilities in identity activities, prevent over classification of the information, and incorporate sharing of identity information with interagency partners.

(b) Globalized threats have increased the need to dynamically and securely share information with allies and partners. Rules for sharing identity data and associated I2 vary widely among North Atlantic Treaty Organization's (NATO's) member states, the United States, European Union (EU), other PNs, and HNs. Additionally, rules for collecting and sharing identity information are influenced by the citizenship of the individual, the reason the data was collected, and the classification level.

(c) When planning for identity activities, commanders consider the military objective but also who else will need the information to support the broader national security goals. Efforts should be made early in the planning process to ensure identity information is usable and interoperable across various multinational systems and at the lowest classification possible.

(3) **Sociocultural Factors.** Joint forces need to demonstrate an understanding of the political, social, economic, and religious dynamics of the OE before executing identity activities. For example, CCDRs should conduct an in-depth sociocultural analysis to identify those cultural attributes of a relevant organization or group, which may pose either short-term or sustained challenges in conducting identity activities. Integrating cultural knowledge and understanding into operations will mitigate potential challenges in identity collection and determine what attributes may be sensitive to the point where they limit collection, where identity information is stored, how it is to be used, or with whom the identity information can/cannot be shared.

(4) **Geographic and Technological Constraints.** During planning, commanders consider the geographic area, environmental elements, and the availability of power generating and communications equipment for forces in the operational area. Utilizing organic communications equipment reduces the time required to transmit, share, match, and verify identity information and is encouraged, as nonorganic equipment may be limited or unavailable in austere operational areas. Commanders should plan for remote operations and determine how to mitigate challenges in collecting and matching biometric data, downloading watchlists, and utilizing DOMEX and forensic reachback capabilities. When conditions warrant, the commander may increase reliance on watchlists or allocate specialized communications equipment (i.e., satellites) to the unit. Remote or maritime operations present challenges to ensure sufficient spare equipment and consumables are available and that the maintenance cycle is responsive. Additionally, austere and remote locations may require planning for the evacuation of certain collected material to preserve, process, and analyze it. The same may be true of units operating afloat enrolling individuals or exploiting materials found on suspect vessels. These units may also have a far more difficult time updating watchlists or taking advantage of available reachback capabilities while simultaneously being the most likely to encounter hostile individuals or networks of interest. The unique challenges of the specific OE should be considered to plan the right mix of equipment and capability to mitigate these challenges, enhance effectiveness, and maintain the ability to match and share the information as quickly as possible.

(5) **Command Involvement.** When units are tasked to conduct identity activities, commanders should emphasize quality and quantity of data collection. Identity activities should be incorporated into unit training, unit exercises, and pre-deployment training as early as possible. When deployed, the command should consider appointing an individual or multiple individuals with the appropriate authority and mix of expertise (e.g., DOD law enforcement; intelligence; explosive ordnance disposal [EOD]; chemical, biological, radiological, and nuclear [CBRN]) to coordinate and direct identity activities and fuse, share, and act upon identity-related intelligence or information. This person(s) should serve as the unit's point of contact for follow-ups, reviewing results of identity collection and exploitation and fusing the data to enhance the overall operational picture, identify gaps or shortfalls in collection and analysis, and with appropriate authority, tasking units to fill any gaps. This construct will facilitate the sharing of identity information with organizations outside the unit.

d. **Operational Design.** Effective integration of identity activities into JPP requires the JFC and staff to understand their capabilities and how to optimize their use. Identity activities should pervade all staff planning processes and elements within JPP. They should be embedded within the operational design of all unit operations and are especially useful in solving ill-defined problems. During operational design efforts, including a focus on individuals who have been linked to enemy locations, events, materials, and networks provides the commander a greater degree of understanding about the complexities of the OE. The commanders' and staffs' understanding of the OE, in turn, enables them to further visualize and integrate identity activities and capabilities into the mission.

5. Capability Needs Across the Phases of an Operation

Identity activities may be conducted in all phases of an operation to directly enable all subsequent phases and support both the intermediate objectives of the phase as well as the strategic objectives of the operation or a separate campaign. The transition between phases is primarily a function of refocusing efforts toward the evolving objectives. The main challenge for planners is to adeptly plan for timely permissions and authorities to allow deployment and fielding of identity activities capabilities that usually require long lead time. Each force provider maintains some level of identity activities capability capacity to support CCDR force requirements. The United States Army maintains the DOD's authoritative biometrics storage and matching repository, a biometrics collection capability, and an I2 production program, as well as deployable forensics collection through tactical forces and exploitation capabilities through the CCMD FXL. The FXL is a full spectrum forensic laboratory accredited to International Organization for Standardization and FBI standards that provides a theater analytic capability in the forensic disciplines of deoxyribonucleic acid (DNA), latent print, firearms and toolmarks, and drug and explosive chemistry combined with intelligence analysis. This combined capability enhances all-source analysis and supports operational decision making. The United States Marine Corps deploys a full biometrics and forensics collection and exploitation suite within a Marine expeditionary force (MEF), and also maintains a web-based data transport and collection management architecture supported by an analytic cell. The United States Navy maintains both a biometric collection capability to support maritime boarding activities and an expeditionary forensics exploitation program focused on EOD support. Additionally, USSOCOM maintains a SOF-unique collection, processing, and exploitation architecture supported by a continuous analytic cell and integrated into multiple interagency partners, including federal law enforcement and the IC. These capabilities are all technically interoperable and capable of supporting a variety of mission applications and activities. The following is a description of the capability planning considerations a JFC should consider.

a. **Shape.** In the shape phase, the command focuses on setting the conditions for successful operations. Shaping activities include long-term persistent and preventive military engagement, security cooperation, and deterrence actions to assure friends, build partner capacity and capability, and promote regional stability. They help identify, deter, counter, and/or mitigate competitor and adversary actions that challenge US security objectives, including national and regional stability. Employing preparatory identity

activities informs operation assessment, planning, and execution to improve the JFC's understanding of the OE.

(1) Identity activities in the shaping phase are largely conducted through other interorganizational participants (e.g., USG departments and agencies, PNs), with DOD in a supporting role. Some partners are quite capable already; others may benefit from assistance. Significant focus on building the identity activities capacity of both forces and MNFs, as well as demonstrating to PNs the value of sharing identity data and other related information to include biometrics, forensics, and document and media collections, will pay dividends over the long-term. A heavy emphasis on collection will also benefit a more fulsome understanding of the OE and its relevant actors. The joint force, in concert with multinational and interagency partners, must maintain and exercise strong regional and HN identity activities partnerships as essential shaping activities in peacetime to ensure operational sharing and collaboration during plan execution.

(2) During shaping activities, CCDRs should task their Service component commands and the CCMD theater special operations command (TSOC) to request collection and, where appropriate, regional or reachback exploitation capabilities to meet their support and military engagement needs. While in some instances a regional exploitation capability will be desired, in most cases reachback capabilities in the continental United States (CONUS) will be sufficient to meet shaping mission requirements. A scalable data and material transport architecture should also be established or assigned to move information and collected exploitable materials from the point of collection to processing and exploitation resources positioned at regional nodes or in CONUS. A sufficient I2 analyst cadre should also be identified and tasked, either through augmented training of existing intelligence analyst staff located at the component commands or JIOCs, formal tasking of a Service intelligence center for I2 production, or via a formal request for forces to stand up a mission-focused analytic cell. USSOCOM provides dedicated analytic support to SOF operating in a joint operations area (JOA).

b. **Deter.** Identity activities support deterrence as part of ongoing operations by identifying possible threats, linkages, and information that can enhance ongoing activities and support preparation for follow-on operations.

(1) Identity activities support both offensive and defensive force enhancements, regardless of the nature of the threat (e.g., traditional or irregular, state or non-state), the threat's actions, or national objectives. Identity activities collection and surveillance activities can create hesitation and doubt within the threat's decision cycle, and I2 products support the refinement of a JFC's CONOPS by informing force protection measures, JIPOE products, predeployment activities, initial deployment into theater, and continued military engagement and sharing with multinational partners.

(2) During deterrence activities, CCDRs should consider increasing their collection assets and corresponding capacity to transport and exploit data and materials. Should combat activities commence, collection can quickly outpace exploitation and analysis capacity creating backlogs and missed opportunities. Planners should consider what prioritization and workflow schemas need to be established and define what

processing, exploitation, and analysis must be completed forward and what can be supported by reachback. This analysis will form the basis for operation order development, formal requests for forces, and joint emerging operation need statements.

c. **Seize Initiative.** JFCs seek to seize the initiative in all situations through decisive use of joint force capabilities. In combat, this involves both defensive and offensive operations at the earliest possible time, forcing the enemy to culminate offensively, and setting the conditions for decisive operations.

(1) The JFC can leverage identity activities capabilities to help degrade the enemy's capabilities, using I2 production to support targeting of key nodes within the enemy's operational and logistics networks and influence other relevant actors within the OE. Using robust knowledge of the human dimension and human-based systems within the OE developed in earlier phases, the JFC can use I2-supported ISR capabilities and I2 and/or DOD law enforcement CRIMINT-focused targeting packages to rapidly apply joint combat power in precise and optimized ways to delay, impede, or halt the enemy's aggression with the intent of resolving the crisis at the earliest opportunity.

(2) Sufficient identity activities collection and in-theater forensic and DOMEX exploitation capabilities should be considered to support operations to gain access to theater infrastructure and expand friendly freedom of action. In areas where the military has not had a long-term presence or does not have a sufficiently willing or capable partner(s), robust and additive collection will be critical to facilitating comprehensive I2 support to military efforts to degrade enemy capabilities in the near to mid-term. USG and military law enforcement relationships with local and regional law enforcement and security organizations should also be leveraged for these purposes. If combat intensifies, planners should consider establishing an identity activities TF to coordinate and manage identity activities assets and information and material flows throughout the AOR. Specific emphasis should be given to determining strength needs and requesting forces related to in-theater and regional exploitation and I2 analysis capability requirements. Planners should also work to develop plans for leveraging identity activities to support ancillary matters beyond offensive operations that will result from increased combat activities, such as internally displaced population management and military detainees. In MNF environments, common data sharing and data/material transport policies, agreements, architectures, and mechanisms should also be finalized. CCDRs should identify and implement guidance and mechanisms to support battlefield evidence requests and applications. Ensuring that sufficient classification, chain of custody, and material preservation and storage guidance is promulgated will be critical to enabling all activities, including potential prosecution, in later phases and even after the current operation or campaign has concluded.

d. **Dominate.** JFCs focus on breaking the enemy's will to resist or, in noncombat situations, to control the OE.

(1) While tactical collection and exploitation activities are not always practical for the conditions of some operations (i.e., large-scale combat operations), identity activities provide meaningful support to large-scale combat activities down to various

stability actions in the form of targeting support, attribution, and force protection. The applicability of this value is largely dependent on the nature of the enemy and the tempo of joint force activities across the OE. If the joint force is constantly on the move (e.g., continuous advancement to the capitol), many identity activities functions may only take place behind the leading edge of the forward advance. However, if combat activities are sufficiently tethered to a specific geographic location (e.g., securing a city or valley), the identity activities operational cycle can still be continuously leveraged to measurable effect.

(2) Within the dominate phase, CCDRs should primarily focus on biometric and material collection and triage and the use of more operationally focused I2 products to inform targeting activities and enhance ISR capabilities. Effective coordination and tracking of MNF and HN collection will also be essential to long-term value. Commander's request for a significant ramp-up of exploitation capacity, both local (in-theater or regionally-based) and reachback, should be anticipated. TF-level leadership and coordination may be required to effectively orchestrate, manage, and maintain the breadth of deployed identity activities assets. Implementing effective case management and records management mechanisms and procedures will also help to ensure that the potential value of collection and exploitation activities is not lost to the turmoil of unit redeployments, leadership changes, and other typical joint task force (JTF) challenges. Furthermore, commanders should seek to identify and implement effective and long-term information management mechanisms capable of operating on an enterprise scale to support broader analytic activities and future mission planning requirements. Working with multinational partners to establish common frameworks and architectures to transport, share, disseminate, and manage identity activities information throughout the OE as well as with national repositories will help to facilitate unity of effort and unified action.

e. **Stabilize.** This phase is typically characterized by the transition from sustained combat operations to conducting and supporting stabilization efforts. There may still be a requirement to support other operations with identity activities during this phase. Within the stabilize phase, JFCs will typically provide supporting capabilities and activities; however, the joint force may be required to perform limited local governance (i.e., military government) and integrate the efforts of other supporting interagency and multinational partners until legitimate local entities are functioning.

(1) Identity activities facilitate efforts to reduce underlying tensions by increasing accountability and supporting effective governance and the rule of law across the plenary of foundational security, essential public service, economic, and political systems. Identity activities capabilities help to mitigate serious internal challenges, such as civil unrest, insurgency, terrorism, and factional conflict, and they can be used to assist stable government's efforts to respond to natural disasters. They also enable the more effective management and administration of humanitarian aid to refugee populations and internally displaced persons. Identity activities can be used to support a broad spectrum of stability activities; from conducting strikes and raids to helping to secure the population and vetting local nationals nominated for sensitive positions or training within HN institutions. They directly support strengthening security organizations, such as

national police and criminal courts, to help legitimize the HN government; and help set the conditions for a political settlement by facilitating an efficient transition toward civil authority.

(2) Within the stabilize phase, commanders should focus first and foremost on robust collection and exploitation activities. Dedicated analytic resources should be established to ensure a consistent stream of I2 production, and should include a scalable DOD law enforcement CRIMINT analytic element. Expeditionary forensic and DOMEX exploitation capabilities should be deployed throughout the theater to meet desired throughput requirements, including robust partnerships with national IC and interagency exploitation centers established and formalized. As stabilization progresses an increased focus on building HN capabilities should emerge to help develop, professionalize, and add legitimacy to HN security and law enforcement systems and processes. Well considered, thoughtful, and routine data sharing practices should be implemented and executed with both the HN and MNF. Such data sharing will likely require a common architectural framework and standards-based approach, but may also necessitate a common enterprise network and security rubric. JFCs should take care to ensure adequate coordination and collaboration with the HN, multinational partners, and interagency partners on all identity activities-related stabilization efforts. Planners should work to ensure key perspectives, plans, and capabilities from the various USG departments and agencies involved are factored into the preparation of identity activities and their execution. Consider including representatives from MNF's militaries and civilian agencies as well as from the United Nations (UN) and other international organizations and nongovernmental organizations (NGOs) should also be included where appropriate.

f. **Enable Civil Authority.** This phase helps, civil authorities regain their ability to govern, administer services, and address other needs of the population.

(1) Identity activities in this phase may be at the behest of HN civil authorities or they may be under their direction, depending upon the level of HN state capacity. They support the civil authority's efforts to provide essential services to the indigenous population, namely security and support to rule of law. Employment of identity activities may require the involvement of interagency partners and may be a supporting element to activities led by other USG departments and agencies.

(2) Within this phase, commanders should focus on identifying the collection, exploitation, and analysis capacity required to support nontraditional military-supported activities, such as repatriation, reintegration, and population management. Strong collaboration with interagency and IC partners in developing and executing collection plans and data management schemas will also help to smooth and diminish redundancy and rework throughout the identity activities operational cycle. Early coordination and decisions regarding who, how, and when collection will be conducted with regards to refugees and internally displaced persons, where that information will be stored, and how it will be made discoverable and/or accessible will mitigate many common challenges throughout the operation. Concurrently, a priority should be placed on establishing, enhancing, or expanding long-term information and collected exploitable material sharing

partnerships with the HN and DOD and its interagency partners. Such efforts can be facilitated through a variety of operational partnerships across the collect, process/exploit, and I2/DOD law enforcement CRIMINT production functions relevant to any of the ongoing operations or activities (e.g., FID, foreign humanitarian assistance [FHA], stability activities, SFA, peace operations). Sharing relationships can also be reinforced through foreign military sales and other partner capacity building activities. These activities should be coordinated with interagency partners through the relevant embassy country team to ensure any capacity building efforts support achievement of objectives. JFCs should also place an emphasis on facilitating the use of collected exploitable materials as battlefield evidence.

6. Additional Planning Considerations

Identity activities are not a new phenomenon within joint operations. JFCs have been employing identity activities since before the Vietnam conflict using the limited capabilities at their disposal; traditionally, to enhance physical security. Today, identity activities are also used to enable safe and effective operations by providing essential information on the adversary and enemy networks, and populations to inform operation planning, execution, and assessment throughout each phase of an operation or campaign. The prevalence and value of information gained by conducting identity activities in today's operations are a function of the exponential increase in technology that has fundamentally changed the way identity information is collected, processed, exploited, and disseminated. These technologies continue to proliferate and often bridge cultural, geographic, and language barriers. Many technologies enable identity activities to be adaptable in a tailorable and scalable approach to support regionally focused missions, bilateral and multilateral military exercises, and security cooperation activities.

a. **Intelligence Support to Planning.** Key considerations for intelligence support to identity activities include constant collaboration among the operations, plans, and intelligence staffs; long-term coordination with PNs; and when necessary, direct access to national intelligence centers and agencies to meet specific requirements. JFC intelligence staffs collaborate with the combat support agencies, USSOCOM, interagency partners, and the IC to build a fused intelligence picture. Distributed identity activities conducted during irregular warfare over a large operational area may require an operations-intelligence fusion capability at the applicable tactical level to ensure that actionable intelligence, which may be perishable, is available to operational commanders in a timely manner. Intelligence support to operations begins with the articulation of mission requirements. This includes identification of information and production requirements to support targeting and PIRs for the commander's decision cycle. For identity activities, commanders should ensure that any requirement for intelligence support to identity activities is identified.

(1) **I2.** I2 utilizes enabling intelligence activities, like BEI, FEI, and DOMEX to discern potential threats by connecting individuals to other persons, places, events, or materials; analyzing patterns of life; and characterizing their level of potential threats to interests. These assessments can be used to characterize the OE; identify threat strategies and COAs; and provide insight into the physical, cultural, and social environments that

influence human behavior. JFCs can exploit biometric, forensic, document and media data collections and integrate that data with other all-source intelligence to locate and track unattributed identities across multiple or disparate encounters, cases, and events, and map out human networks. Commanders should clearly define the focus areas of I2 analysis at each echelon to maximize economy of effort. Roles and responsibilities for I2 production should be assigned from Service intelligence centers and JIOCs/joint analysis centers, CCMD staff, and Service staffs, as appropriate, across TF and brigade intelligence cells, and down to individual unit support elements. Clear guidance and direction will help ensure a sustainable distribution of effort between strategic-theater production (e.g., JIPOE, criminal indictments), operational assessments (e.g., named areas of interest), and tactical support (e.g., watchlisting, warrant support packages).

(2) **Collection Management.** Collection occurs throughout an operation or campaign and across the competition continuum. The JIOC executes collection management authority on behalf of a joint force J-2 and exercises collection requirements management for certain assets and all national resources. In coordination with the J-3, the JIOC delegates or identifies collection management authorities for identity activities for subordinate components and JTFs. Collection managers must know of the capabilities, limitations, survivability, and lead times of available identity activities collection systems, as well as the processing and exploitation, analysis, and production timelines to complete and disseminate, where appropriate, an I2 product or DOD law enforcement CRIMINT product. Collection managers must also be able to coordinate with the J-3 the employment of all available collection capabilities. This includes requesting external theater and national level resources to acquire needed information. Since most identity activities collection will likely be executed by non-intelligence units, the JIOC will need to integrate and coordinate its collection planning with non-intelligence CF and DOD law enforcement units and relevant interagency partners to ensure the broadest level of collection assets are employed to meet the commander's identity activities information needs. Additionally, identity attributes that are collected through military engagements with foreign partners are monitored through a National Security Council (NSC) foreign partner military engagement and governance process. CCMDs who conduct identity data collections through military engagement activities should include them within the CCP and inform the relevant Under Secretary of Defense for Policy (USD[P]) country desk officers of any identity activities-related military engagement planning efforts at the earliest opportunity. Depending on the method of military engagement, DOS approval of the activity may also be required.

(3) **Reachback Support.** Combat operations limit, to varying degrees, the amount and types of forward-located intelligence support provided. As such, identity activities typically benefit from an assigned reachback effort. Reachback capabilities enable forward-deployed forces to leverage national and Service assets outside the operational area for classified and open source research, data, and capability to provide actionable intelligence. Sufficient communications bandwidth and connectivity are essential to reachback support. Interagency partners are a valuable reachback support asset. For example, the FBI's Terrorist Explosive Device Analytical Center (TEDAC) provides national-level exploitation support for IEDs, enabling deployed expeditionary exploitation capabilities to maintain their focus on the commander's time-sensitive

requirements. Similarly, the National Media Exploitation Center (NMEC) provides timely and strategic content analysis of captured documents and digital media. This analysis directly supports theater DOMEX exploitation capabilities to meet operational requirements. Processing and exploitation reachback can also be coordinated through multinational partners who possess similar capabilities. To take full advantage of reachback support, commanders should ensure they have sufficient capacity to transport collected data and materials to reachback processing and exploitation elements. Effective triage protocols should be present to ensure exploitation capacity is not overwhelmed.

b. **Collection.** There are three primary approaches to identity activities collection: collections conducted through foreign information sharing partnerships; HN collections enabled by forces, training, and equipment; and direct collection by forces and MNFs/PNs. In most instances, a combination of two or all of these primary approaches will be used to support military operations. Commanders should remain conscious of the time required to conduct a sufficient collection effort using each approach (or combination thereof) and the impact that will have on supporting exploitation, analysis, and production activities.

(1) Within each operational area, commanders should endeavor to reach a tipping point of collected identities as quickly as possible. A tipping point is the moment at which the required number of unique identities within a given geographic area facilitates a steady stream of repeat encounters of military or intelligence value. The tipping point for each operational area will be different, depending on the threat faced, and will require a different level of effort for collection. For instance, collections in Afghanistan focused mainly on military-aged males and required the collection of approximately 1.8 million unique identities to reach the tipping point. The tipping point in Operation IRAQI FREEDOM only required the collection of 1.1 million unique identities because of the primarily urban nature of the OE. As there is already a large amount of identity data on foreign terrorist operating transnationally, commanders can leverage existing global watchlists to match against threat identities in newer operational areas.

(2) System interoperability between components and PNs is an important consideration. Disparity in data standards can greatly affect the timeliness of data processing activities as well as the future use of the collected data.

(3) Data quality should be a significant priority as it affects processing timeliness and, in some instances, accuracy. The strategic and downstream impacts of poor data quality cannot be understated. Data collected in an operational area through even a single encounter may be used to identify, target, track, interdict, detain, and prosecute threats encountered days, weeks, or years later by DOD components, interagency partners, or select allies operating anywhere in the world. JFCs should require all identity activities-purposed collectors to meet defined training and quality assurance standards, as appropriate.

(4) Certain types of collection activities may require specialized collection teams. These teams may include low density, high skill set expertise and require

significant lead times to be deployed in significant numbers. Commanders should anticipate the need for specialized teams throughout each phase of an operation, and request forces accordingly.

c. **Processing and Exploitation.** Processing and exploitation can be conducted forward in an expeditionary capacity, through reachback capabilities, or a combination of the two. Forward elements may improve timeliness of response but may limit access to relevant information. These capabilities may also be more expensive to operate and maintain in theater. Reachback elements can provide access to more comprehensive and authoritative repositories but require more time to respond to tactical and operational requests. Forward elements will often have lower throughput capacity than reachback elements but will also likely avoid distraction by other organizational requirements and instead focus primarily on meeting the commander's needs.

(1) Command and control (C2) and coordination with non-DOD agencies should be defined early in the planning process. Given the limited capacity of expeditionary elements, multiple force providers serving multiple operational focus areas (e.g., law enforcement, intelligence, C-IED) may seek to deploy expeditionary processing and exploitation capabilities to support the mission. Without sufficient organization C2, and interagency coordination to facilitate unity of effort, these capabilities will likely operate in an unsynchronized, inefficient, and redundant fashion. A clear understanding of C2 relationships, as well as facilitated integration of force provider capability into the JFC's designated TF, will result in more timely and efficient exploitation and minimize the expeditionary element's time to reach full operational capability.

(2) The operational needs met by processing and exploitation capabilities will likely change throughout each phase of an operation. The results of processing and exploitation activities used primarily to support targeting in early phases may be re-used to support prosecution and rule of law activities in later phases. It is incumbent on the commander to organize and direct the commands' processing and exploitation elements to execute their functions in ways that are mutually supportive to the requirements of both activities. This may mean exploitation activities executed to support intelligence operations are conducted anticipating future chain of custody requirements. Similarly, activities conducted to enable detainee processing, management, and prosecution may also need to enable follow-on targeting missions, interviews and interrogations, and source operations.

(3) Common information management and sharing architectures are a vital component of the processing and exploitation function. Follow-on analysis and reference activities require robust, secure, yet accessible, databases that enable ready discovery and usability of processing and exploitation results. Authoritative databases are the best venues for data discovery and data consolidation, making them the most efficient means for data storage.

d. **Sharing of Identity Information, I2, and DOD Law Enforcement CRIMINT.** The effectiveness of identity activities can be enhanced by access to and sharing of identity information, I2, and DOD law enforcement CRIMINT among DOD, interagency,

and multinational partners. Within this context, sharing consists of the transfer of identity information, I2, or DOD law enforcement CRIMINT products, from one organization or system to another. The sharing of identity information, I2, and/or DOD law enforcement CRIMINT products have proven essential to mission success in recent operations. DOD policy states that identity information and materials collected during the course of military operations and activities will be considered DOD data and that that data must be collected, stored, and managed according to approved technical standards; appropriately secured and handled in accordance with published security classification guidance; and shared and/or made available to appropriate mission partners to the maximum extent authorized by law and DOD policy. Given the sensitive nature of identity information and its value to almost any operational effort (including nefarious activities like extra-judicial killings and sectarian violence), commanders must ensure that adequate processes and safeguards are in place to facilitate the sharing and use of identity information and their corresponding I2 and/or DOD law enforcement CRIMINT assessments in legal, responsible, and ethical ways. From the onset of mission planning through the execution of complex operations, commanders and their staffs must recognize and embrace the critical requirement for routinely and continuously sharing identity information and I2 and/or DOD law enforcement CRIMINT products with all appropriate mission partners. Accordingly, commanders at all levels should determine and provide guidance on what information and products need to be shared with whom and when.

See Chapter IV, "Special Consideration," for additional special considerations on sharing identity information, I2, and DOD law enforcement CRIMINT.

e. **Data and Material Transport Mechanisms.** To support identity information sharing activities, DOD has established a comprehensive policy and technical framework to sustain identity activities. This framework encompasses data transmission mechanisms; military engagement schemas; data management policies to facilitate information discovery, accessibility, and use; and designated support organizations to enable and sustain identity activities information sharing from the strategic to the tactical levels. Accordingly, the USG maintains multiple authoritative repositories of identity, forensic, and DOMEX information. These repositories act as strategic assets and capabilities supporting a variety of national security missions and activities across the operations, intelligence, and DOD law enforcement areas. For identity activities to be successful, collected data and materials have to move from the point of collection to these authoritative repositories for processing, comparison, and analysis. There are multiple methods for this movement to occur.

(1) **Web-Based Portal.** DOD maintains web-based portals for transmitting identity data and digitized forensic materials to appropriate entities for processing, comparison, and analysis. These portals are available on both the Non-classified Internet Protocol Router Network and the SECRET Internet Protocol Router Network (SIPRNET), and in some instances, on the NATO battlefield information collection and exploitation system (BICES). When required, the portals can be accessed through an operation-specific Combined Enterprise Regional Information Exchange System capability. The portals are broadly accessible through multiple communication links,

including in some instances, the indigenous communications infrastructure. However, bandwidth issues can be a significantly limiting factor, especially in hostile or uncertain OEs. Planners should ensure the CCMD communications system directorate of a joint staff has granted the authority to operate one or both of these portals on the theater-based network and the appropriate Service-level agreements have been executed with each of the authoritative repository management organizations.

(2) **Dedicated Server Architecture.** A few primary collection systems within the DOD arsenal operate entirely from system-specific infrastructure of servers. These servers operate in a distributed fashion from a central hub, ensuring warehoused data is continuously synchronized with minimal latency. The central hub provides the connection to DOD's authoritative repositories which, in turn, manage automated and semiautomated information exchanges with interagency and other partner repositories. These systems can provide robust support in theaters with a well-developed communications network. However, they can require significant manpower to maintain and service and can display latency in the replication of data being sent forward.

(3) **Dedicated Air Transport.** To support certain missions, commanders may choose to dedicate specific aircraft to collecting and transporting accumulated data and materials to designated theater installations. Dedicated air transport is typically used when timeliness is the critical factor for mission success. However, planners should anticipate potential increases in latency and gaps in the delivery schedule when those aircraft are temporarily re-tasked to support higher priority efforts.

f. **Data Management Policies.** Effective data sharing requires robust data management techniques and procedures. While authoritative repository data stewards will handle the bulk of these efforts, the CCDR retains important responsibilities.

(1) Quality collections are primarily affected by the significance the JFC places on training and routine quality assurance assessments. It is incumbent on operational commanders to stress the status of identity information and material collections as a professional military endeavor to subordinate commanders, staff, and rank and file personnel and to communicate the expectation of high-quality collections appropriately. Commanders should ensure collection activities are included within unit training schedules and predeployment training programs. In-theater support (e.g., technical representatives, field support engineers) should also be leveraged to provide additional unit spot training as needed.

(2) DOD policy requires all biometrics systems to conform to approved standards and specifications. The DOD standard for biometric data is the Electronic Biometric Transmission Specification. Forensic collection and exploitation standards generally mirror civilian law enforcement protocols and procedures, although some are operation-specific and objective-specific in their implementation (e.g., some forensic exploitation conducted to inform intelligence targeting is not required to meet evidentiary standards). Strict adherence to approved standards has a direct positive effect on database quality and processing speed and accuracy. Conversely, loose adherence can create long-lasting data and material processing and management issues and cause

adverse ripple effects throughout the enterprise. Commanders at all levels should enforce the common and complete application of approved standards in all identity collections and activities.

(3) Data collected through CCMD military engagement activities requires thorough review, assessment for veracity, and validation prior to submission to the appropriate authoritative data source for processing and exploitation. While DOD considers all identity information to have operational value, CCDRs should anticipate the myriad downstream DOD and interagency customers that may use that information to support their own national security missions and activities and then make reasonable efforts to ensure erroneous or fraudulent information is not ingested into DOD repositories. Furthermore, if fraud or PN misuse of DOD capabilities is detected, CCDRs immediately inform the appropriate country team(s) and responsible DOD officials (e.g., Defense Forensics and Biometrics Agency, DIA Identity Intelligence Project Office [I2PO], USD[P]).

(4) To facilitate effective data management within the authoritative DOD and interagency repositories, CCDRs must ensure information and materials received from a PN are appropriately tagged prior to submission for processing and exploitation. Tagging should comply with the specifications defined by the appropriate authoritative data stewards and remain consistent across all information and materials provided by the PN.

(5) As part of the formal information sharing arrangement, PNs may request responses/feedback (e.g., match reports, forensic reports, I2 products) for the information, intelligence, and/or materials they submit to DOD for processing/exploitation and analysis. Prior to releasing information back to the PN, JFCs conduct a foreign disclosure review to ensure provided information will not enable misuse or objectionable conduct by the receiving entity. Foreign disclosure reviews should take place for all identity activities information and products regardless of content security classification. However, Defense biometrics, forensics, BEI, and FEI information marked for official use only may be disseminated to representatives of foreign governments and international organizations to the extent that disclosure would further the execution of a lawful and authorized mission or purpose. When possible, JFCs, in coordination with the Under Secretary of Defense for Intelligence (USD[I]) and USD(P), can define common response content and formats that can automatically be released to submitting partners for unclassified information (e.g., red, green, amber responses; limited match reports; tear line alert text). JFCs use Office of the Director of National Intelligence partner or operation-specific guidance and national disclosure policy (NDP) to release classified information.

g. **SOF-Unique Identity Activities Considerations.** Used independently with CF support or integrated with CF, SOF provide strategic options for national leaders and the CCDRs through a global network that fully integrates military, interagency, and international partners. SOF are most effective when special operations are fully integrated into the overall plan and the execution of special operations is through proper SOF C2 elements employed intact. Commander, United States Special Operations Command (CDRUSSOCOM), synchronizes the planning of special operations and

provides SOF to support persistent, networked, and distributed CCDR operations to protect and advance national interests. CDRUSSOCOM exercises combatant command (command authority) over all SOF. CCDRs exercise OPCON over any supporting TSOCs and most often exercise OPCON of SOF deployed in their AORs.

(1) **CDRUSSOCOM** provides direct identity activities support (e.g., training, equipment, exploitation, I2 analysis) to globally deployed SOF and supported CCDRs. Where appropriate, SOF identity activities and capabilities are synchronized and integrated with the identity activities and capabilities of both CF and partners in to achieve unity of effort. The TSOC is the primary theater SOF organization to plan and control special operations and other SOF activities, including identity activities, and is generally responsible for the planning of identity activities executed in support of special operations and the main conduit between USSOCOM and the CCMD.

(2) **I2 Operations.** USSOCOM commonly refers to all SOF use of identity activities capabilities as I2 operations (I2 operations pre-dates the term identity activities). SOF I2 operations combine the synchronized application of biometrics, forensics, and DOMEX capabilities with intelligence and identity management processes. SOF conduct I2 operations under CDRUSSOCOM intelligence authorities as an ISR platform to meet the commander's PIRs. CDRUSSOCOM maintain a full suite of integrated identity activities capabilities and their corresponding management, communication, and partner capacity building architectures in support the full range of global special operations. Military planners should coordinate with their special operations component commands throughout the planning process to determine how best to synchronize and integrate SOF with CF operations to achieve military objectives. Planning staff are cautioned, however, to understand the I2 operations capability architecture is not sufficiently scalable to service the entirety of the joint force for most military operations beyond a certain size. Concurrently, SOF operational requirements cannot be readily met by existing CF capability architectures. Planners should primarily seek to optimize the effective integration of SOF and CF identity activities capabilities by:

(a) Emphasizing unity of effort since unity of command is unlikely;

(b) Establishing policy and procedures to determine which exploitation tier should be leveraged to best meet the broadest range of operational and strategic requirements, given the JFC's priorities and current operational constraints on a case-by-case basis; and

(c) Establishing material management and tasking procedures to take advantage of excess in-theater capacity when operational time constraints require.

See JP 3-05, Special Operations, *for a detailed description of SOF I2 operations. See Chapter III, "Identity Activities Core Capabilities," for more information on forensic exploitation tiers.*

7. Assessment of Identity Activities

Commanders and their staffs must conduct assessments of identity activities as they would any military operation or activity to determine if they are creating the desired effects. Threat networks will adapt visibly and invisibly even as collection, analysis, and assessments are being conducted. Assessments over time that show trends are much more valuable for identity activity planning and operational support than a single snapshot over a short time frame. Over longer periods of time, information can be pieced together, and changes in threat network organization, structure, composition, functions, and operational capabilities can be identified and analyzed. This is particularly valuable for CCP development and in ongoing operations. CCDRs develop their theater strategies by analyzing events in the AOR and developing options to set conditions for attaining strategic end states. When a joint force is employed, it will at a minimum have a baseline of the threat network(s), its characteristics, and behaviors based on shaping operations. Assessment of identity activities is part of the larger operation or campaign assessment and can also support indicator monitoring and measuring effectiveness.

a. Identity activities require a greater application of operational art due to the complexity of the human dimension of the OE. Likewise, identity activity assessments demand staffs conduct analysis more intuitively and consider both anecdotal and circumstantial information. Tactical unit reporting such as patrol debriefs and unit after action reports, when correlated across an OE, may provide the most valuable information on assessing the impact of identity activities.

b. Commanders and their staffs should conduct assessments through a continual process of evaluation and feedback, in which metrics relating to performance and effectiveness of tactics, techniques, and procedures (TTP), systems, and networks are collected and used to assess the entire range of identity activity-related capabilities. This process enables commanders and staffs to improve the performance and effectiveness of identity activities-related capabilities, refine identity data collections, augment I2 production requirements and priorities, and capture best practices and lessons learned. Timely collection, evaluation, and dissemination of observations, lessons, and best practices can specifically influence the next iteration of exploitation or collection activities, avoiding missed opportunities to protect the force or eliminate threats from the OE due to ineffective processes or missed matches against known and discoverable identity data.

c. An identity activity assessment process can take many forms, but all versions typically incorporate four basic tenets: assemble a team of experts to develop indicators, combine different types of indicators to develop a more complete assessment picture, assign weights on multiple axes of the assessment (i.e., by indicator/effect) to ensure that the assessment matches the JFC's priorities, and synchronize assessment timelines so the results flow into higher headquarters' planning processes.

(1) Commanders are encouraged to use a multi-organizational assessment working group approach to develop assessment indicators, which provides the benefit of expert perspectives throughout the staff and subordinate commands, including the

concerns of assigned interagency and MNF personnel. This ensures that the selected questions reflect the priorities of the command and its leadership.

(2) Identity activity assessments should use data from varied sources and employ numerous indicators to ensure the assessment is not dominated by one type of data and represents the full operational view. Additionally, the assessment should measure the full array of identity activities tasks and functions across the operations, intelligence, and law enforcement areas.

(3) The commander should weight each indicator so his most important priorities are reflected in the assessment.

(4) Finally, the assessment process should align to and synchronize with higher headquarters' planning processes, so the assessment results can shape and influence changes in strategy and planning.

d. Integrated successfully, assessment in identity activities will:

(1) Depict progress toward creating desired effects, achieving objectives, and attaining the commander's military end state(s).

(2) Deepen understanding of the OE, JIPOE, and the ongoing intelligence process. Assessments of identity activities can provide additional understanding and greater knowledge about threats and networks, and how operations may be impacting their ability to operate effectively.

(3) Inform commander decision making for operational design and planning, prioritization, resource allocation, and execution. Since identity activities require a high degree of operational art, the contribution of assessments is particularly relevant.

(4) Produce actionable recommendations that inform the commander where to devote resources along the most effective lines of operation and lines of effort.

8. Using Identity Activities to Support Operational Assessment

Commanders continuously observe the OE and the progress of the operation; compare the results to their initial visualization, understanding, and intent; and adjust operations based on this analysis. Staffs monitor key factors that can influence operations and provide the commander timely information needed for decisions. Identity activity capabilities can directly support operational assessment, providing a mechanism to monitor key indicators and measure effectiveness and performance.

a. During execution, assessment actions and indicators help commanders adjust operations and resources as required, such as determining when to execute branches and sequels and make other critical decisions to ensure current and future operations remain aligned with the mission and military end state. Threat networks thrive because of conditions that support their existence and their operations. For example, some threats are supported and concealed by a local populace. However, efficient use of identity

activities can deny a threat anonymity and the ability to blend into society. Additionally, military actions and objectives in the OE can be affected by the actions of a wide variety of entities. These entities include not only the JFC's interorganizational participants but also the civilian population, neutral non-partner organizations in the JOA, and other nations outside the JOA in the CCDR's AOR. Identity activities provide a viable mechanism to identify, assess, and monitor these entities throughout all phases of the operation.

b. Commanders and staffs at all levels develop various operational assessment indicators to track the organization's progress toward mission accomplishment. These indicators include MOEs and MOPs.

(1) The intent in developing MOEs is to identify indicators confirming that military operations are creating desired effects. Identity activities' "hits" can serve as MOE indicators of observable, measurable, system behaviors or capabilities. These indicators help to focus intelligence collection planning. When developed, identity activity-based indicators can inform planning and execution of intelligence collection activities.

(2) MOPs are indicators used to measure a friendly action that is tied to measuring task accomplishment. They are a primary element of battle tracking and are associated with objectives rather than end-state conditions. An example of a MOP is the capture of a high-value target on the DOD BEWL.

(3) Identity activity indicators help commanders and staffs determine whether they are taking the proper actions to attack enemies and networks operating in their operational area. For example, a reduction in the number of foreign fighter encounters often is an indicator of success. Some indicators may be more subjective in nature, however. The willingness of local elders to work with the government and submit their community to identity activity screening is an example of a subjective assessment that requires professional military judgment to determine meaning. It may demonstrate that the threat is exerting less control and fear over the population or it may simply imply a socio-cultural willingness to participate in local security activities. Identity activities can also help monitor indicators of success, such as reductions in a certain tactic employed by the threat network. Enemy shifts in tactics made in response to joint force operations may be a clear indication the JFC is creating the desired effects. Commanders should leverage identity activities to monitor these affects and use them to enhance follow-on planning and decision-making processes.

CHAPTER III
IDENTITY ACTIVITIES CORE CAPABILITIES

"The integration of biometrics and forensic exploitation and especially identity intelligence into national security activities has a tremendous potential to fundamentally change the way we do intelligence at the strategic and operational levels. From uncovering strategic surprise to maintaining global awareness to pursuing terrorists and criminals to securing our borders – these capabilities will form the foundation of our ability to identify and deal with existential threats to national sovereignty in the coming decades."

Herbert Raymond McMaster
Former National Security Advisor, February 20, 2017-April 9, 2018

1. General

a. This chapter describes four identity activity capability sets employed by the JFC to support decision making about individuals of operational or intelligence interest. These capability sets include biometric collection, storage, and matching technologies; forensic material collection exploitation, and preservation processes; DOMEX collection, exploitation, and data management capabilities; and I2 or DOD law enforcement CRIMINT analysis and production.

b. When planning or executing identity activities in support of a military activity or operation, a JFC should identify and leverage all relevant capabilities available to the joint force. Identity activities core capabilities are present and accessible across multiple USG departments and agencies, as well as multiple multinational elements such as NATO, INTERPOL [International Criminal Police Organization] and Europol (European Union Agency for Law Enforcement Cooperation], bearing in mind that both INTERPOL and Europol may have specific policy issues regarding interaction and information sharing with military agencies. Exercising the full extent of these capabilities often requires a coordinated whole-of-government effort, as well as routine collaboration with foreign partners. To effectively exercise such coordination and collaboration, CCMDs must identify, early in the planning process, relevant PN identity programs and activities of concern to the Joint Staff (JS) and the OSD, who can then drive discussions at the national and strategic levels. Concurrently, CCDRs may also use established interagency relationships at the operational and strategic-theater levels to increase their success in identity activities. In each instance, strong collaboration and communication between the CCMDs, JS, and OSD is required to ensure interagency and international support is optimized.

c. JFCs coordinate and cooperate with multinational partners to execute identity activities. With numerous stakeholders involved in identity activities, unity of effort is critical to success and the roles, responsibilities, and authorities of the numerous organizations are understood by the JFC. JFCs should consider the capabilities and responsibilities of the organizations in this chapter when defining command relationships and coordinating interorganizational activities.

2. Biometrics

a. Biometrics is an enabling technology that cuts across many activities and operations and is a key enabler of identity activities. Regardless of disguises, aliases, or falsified documents, an individual's biometrics are unique to one individual and can be attributed to one individual and tracked using various devices and repositories that denies anonymity. Biometrics enhances targeting, security vetting, and force protection by helping to positively identify persons of interest, insurgents, terrorists, criminals, and others who would do harm to force, friendly forces, and facilities. Intelligence-related biometric collections can support or enhance counterintelligence, intelligence analysis, interrogation and detention tasks, high-value target confirmation, source vetting, and attribution, among other activities. MNFs are employing biometrics in operations with increasing frequency and improving results to identify known threats, disrupt adversary freedom of movement within the populace, link people to events, and verify local and third-country nationals accessing MNF bases and facilities. PN and HN laws and social sensitivities must be considered in the establishment of MNF biometric objectives and standards; staff legal, diplomatic, and religious advice can be especially useful in this area.

b. DOD biometric capabilities consist primarily of stationary, man-portable, and untethered collection mechanisms, local and authoritative digital storage systems, and modality-specific as well as fusion matching algorithms. These capabilities are available through each Service and USSOCOM, in addition to the DOD biometrics authoritative source.

(1) The **Secretary of the Army (SECARMY)** is the DOD executive agent (EA) for DOD biometrics, in accordance with Department of Defense Directive (DODD) 8521.01E, *DOD Biometrics.* Within this role, SECARMY leads the requirements, architecture, and standards development efforts for joint, common, and interagency biometric capabilities. SECARMY has designated the Army Provost Marshal General as the responsible official for executing the assignments of the EA.

(a) **Department of Defense Automated Biometric Identification System (ABIS).** The Army's Defense Forensic Science Center (DFSC) operates and maintains the authoritative DOD repository for multi-modal biometrics collected on foreign nationals throughout the course of military operations and shared by PNs and interagency partners, known as the DOD ABIS. The DOD ABIS contains fingerprints, iris scans, facial images, and palm prints collected through direct enrollments, site exploitation activities, direct allied and multinational submissions, and information shared by interagency and foreign partners. This data is normalized and stored in an unclassified repository for comparison against future biometric collections. Through the ABIS, the Army executes the common storage, processing, and matching activities of the DOD biometrics enterprise. The Army also facilitates the systematic sharing of DOD collected biometric data with and from PNs and provides the conduit for matching against interagency authoritative data sets, including dissemination of the DOD BEWL on behalf of DIA.

(b) **Biometrics Automated Toolset-Army (BAT-A).** The Army Program Executive Office for Intelligence, Electronic Warfare, and Sensors maintains the primary multi-modal biometrics collection device for Army units, known as BAT-A. The BAT-A is a man-portable biometrics collection capability that collects fingerprints, facial images, and iris scans, as well as biographic and contextual information relevant to the collection event. BAT-A operates primarily on the SIPRNET and maintains its own server and communications architecture. All BAT-A collected files are transmitted to the DOD ABIS for storage and matching.

(2) **CDRUSSOCOM** provides for all USSOCOM biometric collection capabilities. Handheld multi-modal biometrics collection devices are fielded with every SOF unit and supported by a special operations forces exploitation (SOFEX) architecture. The SOFEX architecture provides a single web-based portal to submit, manage, and respond to all SOF enrollments in near-real time. The SOFEX architecture leverages biometric data and matching capabilities across the USG to support SOF mission planning and execution. All USSOCOM collected files are transmitted to the DOD ABIS for storage and matching. USSOCOM also maintains robust partnerships (often with system-to-system connections) with multiple IC elements and national centers, as well as interagency partners, such as the Department of Homeland Security (DHS) and FBI, which possess forensic exploitation capabilities.

(3) **United States European Command** utilizes a defense exploitation architecture that provides command biometric collection capabilities. Handheld multimodal biometrics collection devices are fielded with every unit and supported by the defense exploitation architecture, which provides a single web-based architecture to submit, manage, and respond to all enrollments in near-real time. All collected files are transmitted to the DOD ABIS for storage and matching.

(4) The **Office of the Chief of Naval Operations (OPNAV)** manages the Navy's Identity Dominance System (IDS) to support the processing of multi-modal biometric information collected from encountered individuals during maritime interception operations. The IDS provides a real-time mechanism to check unknown individuals against the DOD BEWL and support the identification, targeting, and force protection activities of visit, board, search, and seizure (VBSS) teams. All IDS collected files are transmitted to the DOD ABIS for storage and matching. Separately, the NCIS maintains multi-modal biometric collection kits to enable NCIS special agents and Navy Sailors to establish identity, affiliations, and authorizations of known individuals, deny anonymity to threats, and protect personnel, facilities, and assets.

(5) The **Commandant of the Marine Corps** employs a variant of the IDS (Identity Dominance System-Marine Corps [IDS-MC]) collection capability augmented by a variant of the SOF architecture, known as the Department of the Navy Identification and Screening Information System (DONISIS). IDS-MC is a multi-modal identity system that provides a Marine air-ground task force (MAGTF) the ability to collect and submit for matching and storage biometric and related biographic and contextual data in support of operations.

(6) The **Director, DIA** provides biometric capabilities to meet joint force, Service, CCMD, and national IC intelligence requirements.

c. **FBI's Next Generation Identification (NGI).** NGI is a national law enforcement biometric and criminal history system maintained by the FBI's Criminal Justice Information Services Division. NGI provides automated fingerprint, iris, palm, and face search capabilities; latent matching capabilities; electronic image storage; and electronic exchange of biometrics files to more than 18,000 law enforcement agencies and other authorized interagency partners. NGI is the largest criminal fingerprint database in the world, housing the fingerprints and criminal histories of more than 90 million subjects. The DOD ABIS is the primary conduit for submitting and receiving biometric files to and from the NGI.

d. **DHS Automated Biometric Identification System (IDENT).** IDENT is the central DHS-wide system, managed by the Office of Biometric Identity Management, for the storage and processing of biometric and associated biographical information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses. IDENT stores and processes biometric data—digital fingerprints and facial images—and links biometrics with biographical information to establish and verify identities presented at the point of encounter. IDENT maintains more than 230 million biometric files of individuals seeking entry to the United States, which DOD leverages to enhance employment of identity activities.

e. The **IC** maintains multiple classified biometric storage and matching capabilities, some of which are accessible via the Joint Worldwide Intelligence Communication System (JWICS).

f. **National Central Bureaus (NCBs).** Each member nation hosts an INTERPOL NCB, which provides the central point of contact for the General Secretariat and other NCBs. The US NCB is the single USG interface with INTERPOL and is responsible for administering US authorities' access to INTERPOL database. In addition, the US NCB is responsible for seeking the issuance of all INTERPOL notices on behalf of the US authorities, and alerting US authorities to the existence of INTERPOL notices issued by other member nations.

3. Forensics

a. Forensics is the application of multidisciplinary scientific processes to establish facts that can be used by a JFC to support military operations. Forensic disciplines include DNA, serology, firearms and tool marks, latent prints, questioned documents, forensic chemistry, and trace materials. Forensic capabilities can be used to support intelligence functions, operational activities, force protection, HN legal support, and other related efforts. Forensic capabilities aid operations by adding depth and scope to the comprehensive operational picture. Exploited materials can link specific persons to places, materials, or events. The resulting information can provide usable intelligence to

target, attribute, apprehend, and detain or prosecute enemy combatants, terrorists, and criminals.

(1) The **SECARMY** is the DOD EA for non-digital/multimedia forensics, in accordance with DODD 5205.15E, *DOD Forensic Enterprise (DFE)*. Within this role, SECARMY leads the requirements, architecture, and standards development efforts for joint and common non-digital/multimedia forensic capabilities. SECARMY has again designated the Army Provost Marshal General as the responsible official for executing the assignments of the EA.

(a) **The DFSC** provides full-service forensic support (criminal, expeditionary, and reachback) to Army and DOD entities worldwide. The DFSC provides the Services and CCMDs specialized forensic training and research capabilities as well as forensic support to other USG departments and agencies when appropriate. In accordance with DODI 5505.14, *Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders,* DFSC is the DOD program manager for the Convicted Offender DNA Indexing System. DFSC contains two primary elements.

1. The **United States Army Criminal Investigation Laboratory** provides traditional forensic capabilities to support worldwide criminal investigation across all Services.

2. The **Forensic Exploitation Directorate** provides expeditionary and reachback battlefield forensic capabilities to support JFC requirements, to include forensic-related identity activities. The Forensic Exploitation Directorate also provides support to exercises and training as well as CCMD partner capacity building activities.

(b) The **Intelligence and Information Warfare Directorate (I2WD)** provides specialized exploitation capabilities of certain materials collected in an operational area. I2WD primarily provides forensic support to the JFC in the exploitation of foreign materiel and other collected exploitable materials to support science and technology and countermeasure development activities.

(2) The **CDRUSSOCOM** provides for all USSOCOM forensic collection and exploitation capabilities as a SOF-unique military intelligence program. Thousands of forensic collection kits are fielded to SOF organic tactical units and the SOF-unique expeditionary exploitation analysis cells (EACs) in addition to multiple regional exploitation centers, supported by the SOFEX architecture and 24/7 identity exploitation analytical cells. The SOFEX architecture consists of reachback forensic exploitation capabilities resident in TEDAC, I2WD, NMEC, Secret Service, FBI, DIA, and other IC partners to meet mission requirements (e.g., timeliness, national intelligence, special targeting) and support follow-on SOF mission planning and execution.

(3) **OPNAV** manages the Navy's Expeditionary Exploitation Unit (EXU)-1 program to provide advanced expeditionary exploitation capabilities to collect, process, exploit, and analyze improvised and conventional weapons, ordinance, and their

components on both land and sea. The EXU-1 program directly supports weapons technical intelligence activities and C-IED lines of effort, as well as other EOD and countermeasure development efforts.

(4) The **Commandant of the Marine Corps** employs a Marine Corps variant of the USSOCOM expeditionary forensics collection and exploitation capabilities supported by the DONISIS architecture. Each MEF deploys with one or more expeditionary forensics exploitation capabilities (EFECs) assigned under the MEF command element. The EFEC provides task-organized, functionally specialized capabilities that can be tailored to support the operational requirements of the MAGTF commander.

(5) **FBI TEDAC.** TEDAC provides national-level, full-service, exploitation and forensic support to USG entities worldwide. TEDAC provides support for improvised threats to include IEDs and unmanned vehicles. TEDAC coordinates the efforts of the USG, from law enforcement to intelligence to military, to gather and share intelligence about these devices. TEDAC performs IED exploitation using both established and innovative forensic techniques in a high-capacity, multi-agency environment with experienced scientists, engineers, and technicians. TEDAC is a specialized reachback exploitation element of the FBI Crime Lab.

b. The DOD maintains multiple repositories and case management systems for forensically-derived information collected on the battlefield.

(1) **National Deoxyribonucleic Acid Index System (NDIS) and Joint Deoxyribonucleic Acid Index System (JDIS).** Both NDIS and JDIS store and manage digitized DNA profiles. NDIS is limited to DNA profiles collected during the course of law enforcement activities. DNA profiles loaded into NDIS are automatically checked against other DNA index systems connected to the national architecture to support investigations. NDIS data must be collected and used for law enforcement purposes and can only be accessed by law enforcement professionals. JDIS was created as the DOD's intelligence-focused counterpart to the NDIS. JDIS serves as the comprehensive DOD repository for human DNA collected through military operations for intelligence purposes. All JDIS files are presumed non-US persons who may be of intelligence value.

(2) **SOFEX Portal and DONISIS.** Both SOFEX and DONISIS are web-based tools that serve as the submission point and case management system for forensically-derived data and reporting. These systems facilitate the federation of submitted collected exploitable materials across DOD and interagency partners for strategic exploitation and analysis. Responses are either loaded into the portal or a web-accessible link is provided to access exploitation results within another authoritative holding.

c. Forensic exploitation activities are divided into three distinct levels. Each level is described specifically by its depth of exploitation activities and its level of warfare. The levels of exploitation describe function and mission outcome, not organizational primacy or ownership.

(1) Tactical collection and exploitation consist of collection, exploitation, and analysis conducted at the tactical level to provide timely and relevant information to help tactical commanders execute current operations or plan future operations.

(2) In-theater operational exploitation and analysis occurs at the operational level and is used primarily to identify associations between events, people, materials (e.g., improvised weapons; CBRN; conventional weapons).

(3) Out of theater exploitation and analysis reachback provide strategic-theater support and leverages more advanced technical and forensic exploitation and analysis capabilities that usually exist outside of theater. Specialized teams can be deployed to augment in-theater exploitation capabilities. Out of theater also applies to national-level exploitation capabilities that use advanced all-source analysis and scientific techniques to produce products that support national priorities.

4. Document and Media Exploitation

a. DOMEX materials include any information storage media and the means by which it was created (e.g., written, mechanical, chemical, electronic, optical, or magnetic form). A document is any recorded information, regardless of its physical form or characteristics, which contains information to support a range of government and military activities including target development, force protection, intelligence collection, watchlisting, liaison with foreign partners, interrogation, and criminal investigations. Media is any object on which data can be stored magnetically, optically, chemically, mechanically, electronically, or digitally.

b. DOMEX activities can increase the value of information gained, provide timely and relevant information to commanders, support the intelligence and operational decision-making process throughout the competition continuum, and assist judicial proceedings through application of preservation and chain-of-custody procedures. DOMEX may provide information on the strategies, plans, operations, activities, tactics, weapons, personnel, contacts, finances, and logistics of terrorists, criminal networks, and other threats in the OE. DOMEX supports multiple processes, such as intelligence and information generated for future targeting, and biometric and forensic processes supporting the legitimate prosecution of individuals associated to the collected exploited materials. The forensic and biometrics exploitation of captured or acquired documents and media also enables the development of I2 products to support urgent information needs and planning. Exploitation may require the application of several DOMEX capabilities including document exploitation, media exploitation, and cellular phone exploitation.

c. DOMEX is a CCMD responsibility enabled by combat support agency and Service support. The CCMD should include resources for DOMEX capabilities in its planning, programming, and budgeting processes in accordance with DODD 3300.03, *DOD Document and Media Exploitation (DOMEX)*, supported by DIA through the NMEC. DIA staffs and operates theater joint document exploitation centers (JDECs) and

provides other support as needed in accordance with Intelligence Community Directive (ICD) 302, *Document and Media Exploitation.*

(1) **NMEC.** The NMEC coordinates FBI, Central Intelligence Agency, DIA, and National Security Agency efforts to exploit, analyze, and disseminate information gleaned from paper documents, electronic media, videotapes, audiotapes, and electronic equipment seized by the military and IC in operational theaters around the globe. These exploitation and analysis activities can provide valuable insights into the capability, capacity, and intent of threats operating within the OE. NMEC products can be used by I2 and DOD law enforcement CRIMINT analysts to inform detailed assessments and estimates to meet the commander's information and intelligence requirements. DIA serves as the EA for NMEC.

(2) **JDEC.** A JDEC collects and exploits DOMEX materials (e.g., documents, cell phones, and electronic media such as computer files, video) in theater to obtain intelligence. Material exploitation can obtain information on a great range of topics, such as information on enemy and adversary intentions and planning (including deception), locations, dispositions, tactics, communications, logistics, and morale as well as a wealth of information for subsequent long-term exploitation. Exploited materials can support the identification of threats, the mapping of their networks, and inform capability, capacity, and impact assessments of those networks. The resulting I2 products support follow-on strategic and operational planning as applicable.

(3) **Harmony.** Harmony is the centralized repository for foreign military, technical, and open-source documents and digital media of operational and intelligence value and their translations, for the intelligence, national law enforcement, defense, and homeland security communities. Harmony is accessible through multiple secure networks (e.g., SIPRNET, JWICS, Stone Ghost, BICES) and provides a flexible, modular, field-deployable collection tool suite. The Harmony repository is maintained by DIA and is part of the NMEC information technology architecture.

(4) USSOCOM's Joint DOMEX Operations Group collects and exploits collected DOMEX materials (e.g., documents, cell phones, and electronic media such as computer files, video) by providing forward deployed triage teams in theater as well as reachback to obtain tactical and operational intelligence. DOMEX exploitation can obtain information on a great range of topics, such as information on adversary intentions and planning (including deception), locations, dispositions, tactics, communications, logistics, and morale as well as a wealth of information for subsequent long-term exploitation. Exploited materials are shared with NMEC in parallel for strategic exploitation. The resulting I2 products support follow-on strategic and operational planning as applicable.

5. Identity Intelligence and Criminal Intelligence

a. Identity attributes and other information and intelligence associated with those attributes gathered from all intelligence disciplines or law enforcement sources are integrated to produce I2 or DOD law enforcement CRIMINT, as appropriate.

(1) Within the joint force, I2 principally supports the find, fix, exploit, and analyze phases of the find, fix, finish, exploit, analyze, and disseminate process. The JFC receives current identity information and derogatory reporting from all levels of the joint force (including operational, intelligence, and law enforcement elements), the IC, interagency partners, and PNs concerning adversaries, enemies, known or suspected terrorists, foreign fighters, foreign intelligence agents, criminals, opportunists, and other persons of interest. This analysis leverages codified analytic methodologies and compliance with the Office of the Director of National Intelligence analysis standards to produce timely and actionable estimates and assessments to inform the commander's decision cycle. The intelligence generated through all-source analysis of identity activities can take several forms; ranging from graphic displays to traditional reports, disseminated from unclassified to top secret security protocols; in support of a wide variety of military operations and activities.

(2) I2 and/or CRIMINT driven activities combine the synchronized application of biometrics, forensics, and DOMEX capabilities with intelligence and identity management processes to establish identity, affiliations, associations, and patterns of individual and group behavior to deny anonymity to the enemy, adversary, substantiate attribution, inform targeting activities, and protect PN assets, facilities, and forces. These outputs enable tasks, missions, and actions that span the competition continuum. Additionally, BEI and corresponding I2 products support the persistent identification and targeting of threats between and across operations, which enables a range of military and civilian functions.

(3) DOD law enforcement organizations support the collection, processing, and exploitation of identity attributes that enable identity activities. These organizations may also conduct DOD law enforcement CRIMINT analysis and production to support investigations, identify and track criminals, assess criminal informants, and support prosecution activities. DOD law enforcement elements utilize information gathered from law enforcement sources, in a manner consistent with applicable law, to provide tactical and strategic DOD law enforcement CRIMINT on the existence, identities, and capabilities of criminal suspects and organizations.

b. The DIA I2PO is the defense intelligence focal point and advocate for all matters relating to I2, BEI, and FEI. The DIA I2PO provides subject matter expertise to CCDRs and staff on planning, executing, and assessing identity activities; I2 collection management; I2 analysis and production; and partner military engagement activities. The DIA I2PO develops and synchronizes identity collection planning in support of CCMD operational objectives, supports CCMD military engagement and memorandum of cooperation (MOC) development activities, and facilitates DIA's Office of Partner Engagement coordination and approval of I2-related sharing arrangements and agreements. The DIA I2PO also provides direction and oversight for DOD BEWL development, management, and sharing efforts on behalf of the Director, DIA.

See DODI O-3300.04, Defense Biometrics Enabled Intelligence (BEI) and Forensics Enabled Intelligence (FEI), *for additional information about the DIA I2PO.*

c. **Biometric Identity Intelligence Resource (BI2R).** BI2R is an analytic tool set, data repository, and production support system that ingests biometrics and associated intelligence data on biometrically enrolled persons of interest. BI2R disambiguates identity data from multiple systems and networks and pushes correlated data to other intelligence systems to baseline and resolve encountered identities. The system automatically estimates and scores the threat probability for each identity maintained within the system and prioritizes production workflow based on those scores. BI2R is the primary mechanism used to develop and maintain the DOD BEWL.

CHAPTER IV
SPECIAL CONSIDERATIONS

1. General

Within strategic environment, JFCs must plan, execute, and assess identity activities under a range of legal authorities, policy constraints, transnational threats, regional concerns and biases, and most likely within a multinational operational setting.

2. Authorities

Pursuant to US and international law, DOD components have authority to collect, process, and exploit identity information, forensic materials, and captured materials. These activities, however, may be subject to limitations, restrictions, or conditions on collection and data use depending on the circumstances (time, place, manner, and purpose) of the activity. Identity activities may be conducted during times of peace or conflict; at home, abroad, or on the high seas. The collection may be obtained through a variety of means and methods, and the identity information may be used for a variety of purposes supporting operations. Additionally, in certain circumstances, a JFC may choose to apply or conform to HN law. JFCs and their staffs must be cognizant of these circumstances and assess their legal impacts (restrictions, limitations, or conditions), if any, on the operation and the identity activities conducted to support it. In each instance, commanders should seek the counsel and recommendations of their operational law SJAs to ensure the legal sufficiency of their actions.

a. **Law of War.** In accordance with DOD policy, DOD personnel comply with the law of war during all armed conflicts; however, such conflicts are characterized, and in all other military operations. For more information, see DODD 2311.01E, *DOD Law of War Program.* Identity activities must fit within the scope and authority of the mandate that authorizes the operation (e.g., Presidential directive, congressional authorization to use military force, UN Security Council resolution, and/or general principles of self-defense [UN Charter Article 51]). The law of war traditionally regulates the resort to armed force, specifically, the conduct of hostilities and the protection of war victims in both international and non-international conflict, belligerent occupation, and the relationships between belligerent, neutral, and non-belligerent states. It is derived from the Hague Convention, treaties, Geneva Conventions, and customary international law with the intent to protect combatants, noncombatants, and civilians from unnecessary suffering, provide certain fundamental protections for persons who fall into the hands of the enemy, facilitate restoration of peace, assist military commanders in ensuring the disciplined and efficient use of military force, and preserve the professionalism and humanity of combatants. The routine means and methods of conducting identity activities that are necessary to obtain information about the enemy and their country is considered permissible during armed conflict. While permissible, the law of war may, however, restrict the employment of identity activities. For example, the taking of a facial photograph of a prisoner of war (POW) for identification may be authorized, but the publication of the photograph in a newspaper, thereby exposing the POW to insults and public curiosity, is prohibited under Article 13 of the Third Geneva Convention.

b. **Law of the Sea.** Within the maritime domain, the conduct of identity activities is principally challenged by the circumstances of the activity. During times of conflict or hostilities, employment of identity activities will be guided by the law of war, UN Security Council resolutions, and ROE. During peace time, different laws apply depending on the physical location (e.g., internal waters, territorial waters, archipelagic waters, contiguous zones, or the high seas) where the activity is being conducted. Rules pertaining to innocent passage, transit passage, and sovereign immunity may affect collection and use. Different rules also apply depending on the types of operations being conducted (e.g., approach, visits, searches). Under these rules, certain classes of individuals (e.g., foreign naval personnel) may be specifically protected. Specific case-by-case authorizations may be required prior to conducting identity activities depending on the circumstances.

For more information, refer to Navy Tactics, Techniques, and Procedures (NTTP) 3-07.11M/Coast Guard Tactics, Techniques, and Procedures (CGTTP) 3-93.3/Marine Corps Interim Publication 3-33.04, Visit, Board, Search, and Seizure Operations.

c. **Geneva Conventions and UN Declarations**

(1) The four Geneva Conventions of 1949 apply as a matter of international law to all military operations that qualify as international or non-international armed conflicts and cases of partial or total occupation. These treaties are intended to provide comprehensive humanitarian standards for the treatment of POWs and detainees, and the protection of civilians without adverse distinction. Commanders must ensure the employment of identity activities complies with the Geneva Convention treaties, most notably in the treatment of POWs and the protection of civilians in a time of war.

(2) Certain identity activities may be broadly interpreted within the UN's Universal Declaration of Human Rights as subjecting individuals to arbitrary interference with their privacy. However, it should be noted that legitimate interference is clearly permitted within international law (e.g., EU law) by a state interested in enforcement of the just requirements of morality, public order, and the general welfare. As such, JFCs are traditionally authorized to obtain and use identity information for legitimate purposes as a matter of public order or general welfare, which include national security, in both international and non-international armed conflict situations.

d. **HN Law**

(1) The desire to conduct identity activities within an HN's borders during peace time (e.g., to enhance protection of overseas installations and personnel) will require compliance with HN law. Commanders should coordinate with their assigned legal advisor and the country team to review HN law as well as pertinent agreements between DOD and the HN (e.g., defense cooperation agreements, status-of-forces agreements). The appropriate senior defense official/defense attaché (SDO/DATT) should have situational awareness of all identity activities being conducted within the HN and accessibility to HN personnel knowledgeable about their requirements and process

for admitting identify information and collected evidence from exploitable materials into their courts of law.

(2) HN law governing an individual's right to privacy could significantly affect how and what identity activities can be employed during a military operation: limiting certain uses, requiring specific handling conditions for identity information, and/or restricting the means of collection.

3. Legal and Policy Considerations

Identity activities are likely to involve a myriad of legal and policy considerations. Because of the nature and complexity of the operational legal issues involved (e.g., law of war, ROE, RUF, detainees, dislocated civilians, negotiations and involvement with local and HN governments), the assigned legal advisor should be consulted early and frequently throughout identity activity planning and execution.

a. **The Privacy Act.** The Privacy Act (Title 5, United States Code [USC], Section 552a) prescribes how USG departments and agencies are to maintain (defined as maintain, collect, use, or disseminate) identifying information (record) about a US person (citizen or legal permanent resident). A record is identified as any item, collection, or grouping of information about an individual to include biometric, biographical, or other identifying data. The Privacy Act does not apply to non-US persons or non-living US persons; however, the Privacy Act does apply to combatant and noncombatant US persons. The Privacy Act generally affords an individual for whom an agency maintains information notice that the agency has the record, access to see the record, ability to consent to the sharing of the record, and ability to submit a letter of disagreement about the information maintained. Military units that encounter individuals who claim to be or are believed to be US persons may be required to provide certain notifications (e.g., Privacy Act statements) and/or specifically manage collected information in compliance with the Privacy Act. JFCs who believe they may have collected personally identifiable information on a US person or are operating in an area populated with US persons should consult their SJA for guidance on Privacy Act requirements.

b. **The Posse Comitatus Act (PCA).** PCA (Title 18, USC, Section 1385) and DOD policy restricts the use of Army, Air Force, Navy, and Marine Corps personnel from engaging in direct civilian law enforcement or regulatory functions absent specific exceptions. The PCA and DOD policy applies to activities within the United States and any territory or possession of the United States or any political subdivision thereof. JFCs planning to conduct identity activities within the United States should consult their legal advisor for guidance on PCA restrictions and if proposed identity activities are permissible.

c. **Leahy Vetting Requirements.** The Leahy Amendments (Section 620M of the Foreign Assistance Act of 1961 codified in Title 22, USC, Section 2151n) prohibit the USG from providing funds to a unit of the security forces of a foreign country if DOS has credible evidence that the unit has committed gross violations of human rights. The provisions restrict funding until the Secretary of State determines and reports that the

government of such country is taking effective measures to bring the responsible members of the security forces to justice. Title 10, USC, Section 362, prohibits DOD from using departmental funds for any training, equipment, or other assistance to a unit of a foreign security force if SecDef has credible information that the unit has committed a gross violation of human rights. Consistent with US law and DOD policy, all SSA activities, and some intelligence collection operations, related to identity activities will require Leahy vetting before they are implemented.

d. **National Policy Considerations**

(1) **Executive Order (EO) 12333, *United States Intelligence Activities.*** EO 12333 regulates the use of national intelligence assets. Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers and their agents, threat organizations, and actors is essential to informed decision making in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and should be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and is respectful of the principles upon which the United States was founded. JFCs collect information through identity activities and conduct identity activities to protect against international terrorism, proliferation of weapons of mass destruction (WMD), foreign intelligence activities, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents in accordance with priorities set by the President. This information must be collected, managed, shared, and used pursuant to the authorities and restrictions of the Constitution, applicable law, the policies and procedures authorized in DODD 5240.1, *DOD Intelligence Activities,* and other relevant DOD policies authorized by USD(I). Special emphasis should be given to the protection of the constitutional rights and privacy of US persons.

See DODD 5240.1, DOD Intelligence Activities, *for more information.*

(2) **Presidential Directives**

(a) **National Security Presidential Directive (NSPD)-59/Homeland Security Presidential Directive (HSPD)-24, *Biometrics for Identification and Screening to Enhance National Security.*** The use of biometrics improves DOD's ability to identify and screen persons for whom an articulable and reasonable basis for suspicion exists that they pose a threat to national security. The directive instructs all federal agencies to make available to other agencies biometric and associated biographical and contextual information associated with such persons. NSPD- 59/HSPD-24 identifies the importance of collecting and sharing identity information across USG departments and agencies and has provided a foundation to apply biometrics technologies to the collection, storage, use, analysis, and sharing of identification data.

(b) **HSPD-6, *Integration and Use of Screening Information to Protect Against Terrorism.*** To protect against terrorism, it is the policy of the United States to develop, integrate, and maintain thorough, accurate, and current information about

individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and use that information as appropriate and to the full extent permitted by law. Operational commanders shall, on an ongoing basis, collect and provide all appropriate identity information on terrorists encountered in the OE to the National Counterterrorism Center through the DIA Watch Listing Division.

(c) **NSPD-33/HSPD-10, *Biodefense for the 21st Century*.** The United States places special emphasis on the need for proactive steps to confront biological weapons threats. Consistent with this approach, DOD is focused on detecting and, when possible, destroying an adversary's biological weapons assets before they can be used. The use of identity activities further expands existing capabilities to interdict enabling personnel, technologies, and materials, including through the Proliferation Security Initiative, and enhances supporting intelligence capabilities to provide timely and accurate information to enable proactive prevention. Early detection, recognition, and warning of biological threats and weapons proliferation networks permits timely responses at the tactical, operational, and strategic levels to deter their use, inhibit their movement, and mitigate the potential consequences of their activities. Deterrence is the historical cornerstone of biological weapon defense, and attribution—the identification of the perpetrator as well as the method of attack—forms its foundation. Biological weapons lend themselves to covert or clandestine attacks that permit the perpetrator to remain anonymous. Continuous use of identity activities enhances the deterrence posture by improving attribution capabilities through technical forensic analysis and I2 attribution assessments.

(d) **Presidential Policy Directive (PPD)-18, *Maritime Security Policy*.** Due to its complex nature and immense size, the maritime domain is particularly susceptible to exploitation and disruption by individuals, organizations, and states. The maritime domain facilitates a unique freedom of movement and flow of goods while enabling people, cargo, and conveyances to transit with anonymity not generally available over land or by air. Individuals and organizations hostile to the United States have demonstrated a continuing desire to exploit such vulnerabilities. Under its existing authorities, DOD deploys its full range of operational assets and capabilities to prevent the maritime domain from being used by terrorists, criminals, and hostile states to commit acts of terrorism and criminal or other unlawful or hostile acts against the United States, its people, economy, property, territory, allies, and friends. JFCs execute identity activities, consistent with US law, treaties, and other international agreements, to enhance the security of and protect US interests in the maritime domain, including, but not limited to, countering terrorist travel, conducting counter-piracy operations, interdicting illicit traffickers, and enhancing maritime domain awareness.

(e) **PPD-23, *Security Sector Assistance (SSA)*.** The United States shares security responsibilities with other nations and groups to help address security challenges in their countries and regions, whether fighting together in a multinational environment; countering terrorist or international criminal networks; participating in international peacekeeping operations; or building institutions capable of maintaining security, law and order, and applying justice. Multiple USG departments and agencies contribute to SSA,

but unity of effort across the USG is essential. For this purpose, the United States applies a whole-of-government approach to planning, synchronizing, and implementing SSA to ensure alignment of resources and national security priorities. This approach applies to identity activity military engagement activities. CCDRs seeking to provide PNs with identity activity-related articles, training, or services should consult the Defense Security Cooperation Agency and seek DOS review and approval as required.

See JP 3-20, Security Cooperation, *and the* Defense Security Cooperation Agency Security Assistance Management Manual, *for more information.*

(3) ICDs

(a) **ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*** The Director of National Intelligence has established guidelines that address mandates in the Intelligence Reform and Terrorism Prevention Act of 2004 to strengthen the sharing, integration, and management of information within the IC, and established policies for discovery and dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC. The overall objectives of this policy are to foster an enduring culture of responsible sharing and collaboration within an integrated IC; provide an improved capacity to warn of and disrupt threats to the US homeland, US persons, and US interests; and provide more accurate, timely, and insightful analysis to inform decision making by the President, senior military commanders, national security advisors, and other executive branch officials. To this end, JFCs shall treat identity information collected and I2 analysis produced as national assets and, as such, shall act as information stewards who have a predominant responsibility to provide. In addition, authorized IC personnel have a responsibility to discover identity information and I2 believed to have the potential to contribute to their assigned mission need and a corresponding responsibility to request the relevant identity information and I2 they have discovered. Commanders are responsible for the proper handling and use of information received from a steward. All discovery, dissemination, retrieval, and use of identity information or I2 collected, analyzed, or produced shall be consistent with applicable law and in a manner that fully protects the privacy rights and civil liberties of all US persons, as required by the Constitution, US law, EOs, Presidential directives, court orders, and Attorney General-approved guidelines, including those regarding the dissemination of US person information, and consistent with the Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment.

(b) **ICD 302, *Document and Media Exploitation*.** DOMEX is the processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under the USG's physical control. DOMEX is a core component of identity activities, providing critical insight into the capability, capacity, and intent of threats and networks. DOMEX serves to illuminate behavior, patterns of life, associations, and the potential level of knowledge and expertise of threats encountered in the OE. Acknowledging the importance of DOMEX activities and capabilities, the DNI has established the NMEC to advance the IC's collective DOMEX

capabilities and ensure prompt and responsive DOMEX support to the JFC and subordinate elements.

e. **NDP.** NDP governs the disclosure of US classified military information to foreign governments and international organizations. While identity information is normally unclassified, certain conditions (e.g., method or source of collection) can cause the information to be classified confidential or above. Similarly, most I2 is classified according to derivative classification rules established in Department of Defense Manual (DODM) 5200.1, *DOD Information Security Program*, Volumes 1-4. However, certain I2 products (e.g., subsets of the DOD BEWL) can be promulgated at the unclassified/for official use only level. Identity information and I2 is useful only when it is provided to those who can act on it, and in many cases that includes foreign allies and PNs. For this reason, identity activity-related information and I2 products should be developed and maintained in a manner that facilitates the broadest degree of responsible sharing whenever possible.

f. **DOD Policy Considerations**

(1) **DOD Issuances**

(a) DODD 8521.0E, *DOD Biometrics*, establishes policy and assigns responsibilities for DOD biometrics. The DOD biometrics enterprise provides a critical end-to-end capability through a defined operations-intelligence cycle to support tactical and operational decision making across the competition continuum for DOD warfighting, intelligence, law enforcement, security, force protection, homeland defense, counterterrorism, business, and information environment mission areas. The DOD biometric and intelligence enterprises are integrated and interoperable through the use of I2 capabilities, including BEI, to the fullest extent possible to enable DOD and mission partners' operations.

(b) DODD 5205.15E, *DOD Forensic Enterprise (DFE)*, establishes policy and assigns responsibilities within DOD to develop and maintain an enduring, holistic, global forensic capability to support the full competition continuum. The DOD forensic enterprise consists of those DOD resources, assets, and processes that provide forensic science analysis linking persons, places, things, and events. The directive designates the SECARMY as the DOD EA for those forensic disciplines relating to DNA, serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, and trace materials, as well as forensics relating to forensic medicine disciplines such as forensic pathology, forensic anthropology, forensic toxicology, and DNA analysis to identify human remains. It further designates the Secretary of the Air Force as the DOD EA for digital/multimedia for those forensics' disciplines relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis.

(c) DODD 3300.03, *DOD Document and Media Exploitation (DOMEX)*, establishes policy, assigns responsibilities, and provides direction for DOD DOMEX in accordance with DODD 5105.21, *Defense Intelligence Agency (DIA)*, and ICD 302, *Document and Media Exploitation.* The processes for collection, analysis, and

dissemination of DOD DOMEX-derived information shall be integrated into military planning and execution at all levels; use standardized methods of collecting and processing documents and media captured or otherwise acquired during DOD operations; focus on rapid and broad dissemination of both raw data and finished exploitation products to tactical, operational, strategic, and national customers; and utilize the NMEC as the central DOD clearinghouse for processing DOD-collected documents and media.

(d) DODD 5240.1, *DOD Intelligence Activities*, and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*, set forth the conditions under which DOD can conduct intelligence activities, including when DOD intelligence assets may collect and retain information on US persons. Within the limits of the law, DOD may collect and retain information on US persons reasonably believed to be engaged in foreign intelligence or terrorist activities, among other reasons set forth in Procedure 2 of DOD 5240.1-R. Because of the numerous legal restrictions placed on the collection of intelligence against US persons, all intelligence activities must be coordinated with the servicing SJA before execution.

(e) DOD 5400.11-R, *Department of Defense Privacy Program*, provides guidance on Section 552a of Title 5, USC, the Privacy Act of 1974, as amended, and prescribes uniform procedures for implementation of the DOD Privacy Program.

(f) DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*, establishes general policy, limitations, procedures, and operational guidance pertaining to the collection, processing, storage, and dissemination of information concerning persons and organizations not affiliated with the DOD. This directive prohibits collecting, reporting, processing, or storing identity information on individuals or organizations not affiliated with the DOD, except in those limited circumstances where such information is essential to the accomplishment of DOD missions. Several core DOD identity activity capabilities have been granted an exception to this policy.

(g) DODI O-3300.04, *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI)*, establishes DOD policy and assigns responsibilities for management and execution of BEI and FEI and support to I2 activities. Additionally, it establishes the I2PO within DIA to coordinate and synchronize BEI and FEI activities. Effective BEI and FEI are an integral part of the DOD biometric and forensic enterprises and are strategically important identity activity intelligence processes used to unambiguously identify persons, networks, and populations of interest who pose potential threats to US forces and national security.

(h) DODI 5525.18, *Law Enforcement Criminal Intelligence (CRIMINT) in DOD*, establishes DOD guidelines and principles for the collection, analysis, and distribution of DOD law enforcement CRIMINT within and externally to DOD in accordance with the National Criminal Intelligence Sharing Plan. The purpose of DOD law enforcement CRIMINT activities is to prevent crime and aid enforcement objectives identified by DOD law enforcement agencies. This is done by gathering information from sources, in a manner consistent with the law, to provide tactical and strategic law

enforcement CRIMINT on the existence, identities, and capabilities of criminal suspects and organizations and to establish policy to prevent crime and aid enforcement objectives identified by DOD law enforcement agencies.

(2) **OSD Memorandums.** In accordance with OSD memorandums, the CCDRs and the Secretaries of the Military Departments are authorized to employ DOD biometric capabilities in concert with our PNs to meet the full range of mission requirements, as permitted by law. The use of international partnerships for biometric information collection in various manners, including leading and/or assisting in biometric collection efforts in PNs and acquiring information from a PN under a sharing agreement is authorized. The categories of non-US persons from which biometric information can be collected, stored, enrolled, shared, and analyzed are:

(a) Persons encountered during maritime interception operations.

(b) Persons detained under the law of war or pursuant to military operations.

(c) Persons of interest.

(d) Local employees.

(e) Third-country nationals.

(f) Non-US persons seeking access to DOD facilities and installations.

4. Multinational Operations

US commanders should expect to conduct identity activities as part of an MNF conducting military operations. These operations, which could occur in a formal multinational alliance or a less formal coalition, could span the competition continuum and require coordination with a variety of other interorganizational partners. To effectively employ identity activities, commanders and staffs must be cognizant of differences in partners' laws, doctrine, organization, equipment, terminology, culture, politics, religion, and language, to craft appropriate solutions to achieve unity of effort. Multinational considerations also include international law, agreements, arrangements, and national laws and caveats required to protect the sovereign interests of troop-contributing nations.

a. Whenever possible, identity activities should include participation by the HN and multinational partners. Multinational partners may possess robust collection, processing, exploitation, and intelligence resources, or at least niche capabilities that may provide invaluable access and insight regarding particular aspects of the OE. Many of these nations may also have extensive regional expertise based on their historical experience.

b. When conducting identity activities that involve interaction with nonmilitary organizations, it is important to consider the ramifications of labeling identity information or releasable I2 products as intelligence. In many cultures, the perception of intelligence

connotes information gathered on an HN citizenry for coercive purposes. Furthermore, attempts to exchange information with many NGOs and international organizations may prove difficult. Most NGOs and international organizations are eager to maintain political neutrality and are unlikely to associate with any overt or perceived intelligence gathering activities. Nevertheless, identity information and I2 product exchange throughout the operational area for the purposes of fostering mutual interests in resolving or deterring conflict or increasing security is highly beneficial to all concerned parties. All information exchange should comply with US law and DOD security guidelines.

c. For military operations, the responsibility and authority for using military force is generally delegated from the President through SecDef to the supported JFC in the form of approved plans/orders with either ROE for operations overseas or RUF. When compared to large-scale combat operations, ROE for limited contingency operations may be more restrictive and detailed, especially in an urban environment, due to national policy concerns for the impact on civilians, their culture, values, and infrastructure. A JFC may begin operations with different ROE/RUF for each type of mission or activity, which may affect employment of identity activities capabilities. When planning identity activities, the JFC and staff should determine what authorities and permissions are required, including anticipating the need for changes based on changing conditions, evolution in the phases of an operation, and branches/sequels to a plan. Depending upon the required level of approval, the JFC must take anticipatory action if the changes are to be timely enough for effective operations. When conducting identity activities in a multinational environment, the use of identity activity capabilities may be influenced by the differences between US and HN or PN ROE/RUF. Commanders at all levels should consult with their assigned legal advisors and take proactive steps to ensure the individual Service member understands the current ROE because a single errant act could cause significant adverse diplomatic/political consequences.

d. The joint force will typically operate in a complex international environment alongside other organizations that will have a need for identity information and I2 products. They are also likely to possess valuable information they can provide the joint force that is unique to their own mission and sources. The sharing of identity information, while often unclassified, requires careful control and assessment, continuously weighing the benefits of sharing against the possible risks of data compromise and the potential for unintended use of US-provided information. Concurrently, the data provided by a PN, if false or inaccurate, may have far-reaching and strategic impacts on a broad variety of national security activities. The JTF J-2 and/or CCMD J-2 must have a process in place to responsibly exchange information with external sources and assess the validity of information supplied by mission partners. This process should include foreign disclosure officers with sufficient training and experience in sharing identity information and the proper authority to disclose classified I2 products to foreign governments and international organizations in accordance with legal and policy guidelines. Mission partners may include USG interagency members, UN organizations, PNs, allied military and security members, local indigenous military and security forces, NGOs, and private companies and individuals providing contract services within the operational area. Although the joint force may have organic identity activity

capabilities assigned, these mission partners may provide the bulk of collection, processing, and exploitation capabilities.

e. Multinational organizations such as INTERPOL, Europol, and NATO can be key partners in the employment of effective identity activities to maintain and employ identity activities capabilities to support their operations and constituents. While these capabilities may be robust, commanders should understand the legal, political, and cultural frameworks under which they have been established and can be employed well before forces are deployed to ensure all the necessary agreements, arrangements, and procedures are in place to support effective collection, processing, exploitation, data sharing, storage, and use. Similarly, commanders should ensure they understand and have adequately planned for differences in the technical standards, TTP, and communications architectures required to interoperate with these strategic partners. The USG may have multiple relationships and agreements with these organizations that must be thoroughly considered and respected to avoid confusion, overlap, and the potential for unintended diplomatic/political consequences.

f. A multinational identity activities effort requires interoperable data and data exchange capabilities. Whenever possible, participants should agree to work from a standard collection and transmission specification to facilitate interoperable processing and exploitation. A multinational identity activities plan should address how all data will be shared between member forces, including disclosure and release procedures for I2 information and products. The CCDR should work to standardize data schemas, operating procedures, and TTP prior to the need to deploy to a combat zone and regularly test these arrangements during multinational exercises. This construct enables PNs to effectively institutionalize these factors into their traditional training, doctrine, and employment mechanisms. DOD has established approved data and transmission standards for multiple capabilities that enable identity activities. It has also ratified biometric standards and BEI reporting formats within NATO policy. All of these approved standards are based upon current published national standards.

5. Sharing of Identity Information, Identity Intelligence, and Department of Defense Law Enforcement Criminal Intelligence

a. The amount of identity information or I2 and/or DOD law enforcement CRIMINT products required to be shared varies widely based on the nature of the military operation. In general, combat operations with MNFs require much more robust information and intelligence sharing than humanitarian or peacekeeping operations. The JFC should scale the organization's capability to share identity information, I2, and DOD law enforcement CRIMINT products, accordingly.

b. Information sharing activities should be planned to leverage identity activities capabilities; facilitate collaboration; support unity of effort; and facilitate achievement of objectives. The strength and effectiveness of identity activities are loosely linked to the size and completeness of its accessible framework of authoritative data sets. The utility of identity activities is greatly reduced if new data is not promptly integrated with existing data sets, which must be routinely and continuously enhanced through direct

enrollments, encounters, and collections; robust interagency partnerships; aligned allied programs; and military engagements. When initiating operations in a new theater, collections are more likely to be matched against existing interagency and/or allied data sets than existing DOD holdings. Collected materials are more readily exploited, sourced, and attributed if there is an appropriately sized library of samples available for comparison. New threats can be identified, even before deployment if strong data sharing partnerships are formed and actively nurtured with PNs. Regardless of the mechanism, dynamic information sharing activities are the cornerstone to ensuring that authoritative data sets contain the breadth and depth of information needed to support operational activities in any AOR around the globe.

c. CCDRs also increase DOD's accessible data holdings through military engagements. These activities facilitate and strengthen data sharing relationships to broaden USG access to operational identity information that may be out of the reach of forces. As appropriate, each CCMD has established an office to manage the employment of identity activities to support the CCMD's mission. These offices, in coordination with the JS J-5 [Strategy, Plans, and Policy], DIA I2PO, and the appropriate USD(P) country desk officers plan and execute military engagements to gain access to and collect foreign partner data on relevant actors.

(1) To support the CCDR's military engagement efforts, OSD has approved a template to facilitate the negotiation of formal identity data sharing arrangements with foreign partners. These arrangements are planned and negotiated by the CCDR, endorsed by the appropriate chief of mission (COM), and approved and/or executed by the appropriate assistant secretary of defense within USD(P). CCDRs may seek to develop MOCs with PNs to share information, ensure technical interoperability and operational congruence during future multinational operations, and/or to support independent PN activities that support CCDR objectives. The resulting nonbinding MOC provides a long-term mechanism with which to guide mutually supportive collection efforts, support distributed counter threat network activities, align PN interests, and increase regional security all while increasing the size and quality of the authoritative reference data sets applicable to various CCMD missions and theaters.

(2) CCDRs follow an ordered military engagement process that begins with including targeted military engagements within the CCPs and the relevant integrated country strategies. Identity activities-related military engagements can range from simple bilateral data sharing arrangements to security cooperation (e.g., train and equip) activities that involve multiple interagency partners and/or NSC approval. Regardless of the desired objective, CCDRs must work through the JS J-5 country officer to inform and coordinate with the USD(P) country desk as early as possible in the planning stages. This will help to ensure CCMD identity activities engagements support DOD and national foreign policy objectives and do not run afoul of the NSC foreign partner military engagement governance framework described below. Each military engagement proposal must also be reviewed for legal sufficiency by the CCMD legal counsel and, if appropriate, the DOD Office of General Counsel for International Affairs. PN identity activities security cooperation and data sharing activities must comply with both and HN laws and regulations. In addition to DOD reviews and approvals, CCDRs must

coordinate with the appropriate embassy country team(s) to gain COM approval for the proposed military engagement. The CCMD entry point for the embassy country team is the SDO/DATT, who should have situational awareness of all identity activities being planned or executed by, with, through, or within the HN. CCDRs should request a foreign partner viability assessment from the country team to inform military engagement planning once the initial concept proposal is complete. COM approval should not be sought until the country team has completed this assessment. CCDRs may execute identity activities-based military engagements upon the concurrence of the USD(P) and the approval of the COM.

(3) To facilitate integration and synchronization of USG prioritization, military engagement, and sharing activities, the NSC has established an international governance framework for identity information. The implementation plan provides a whole-of-government approach to leverage USG department and agency activities to build strategic partnerships with PNs and increase the mutual national security benefit of these activities. It establishes a coordination mechanism to ensure foreign partner military engagements are integrated, synchronized, and deconflicted, as appropriate, and executed in accordance with national security objectives. In accordance with this plan, CCDRs, through the USD(P), shall provide the national security community sufficient visibility into their military engagement activities to ensure each effort serves the broadest range of USG interests, avoids the inadvertent loss of capability and/or confusion by PNs, prevents duplication of effort, and fully considers any foreign policy objective-based issues and reservations.

(4) Standardization impacts DOD's ability to share identity information with foreign partners. To avoid the negative operational effects and costs associated with translating and reformatting identity data, CCDRs are encouraged to address the receipt and processing of identity data for each nation within their AOR in their CCPs. Additionally, CCDRs must consider the interoperability of chain-of-custody standards, systems, and data both between their foreign partners and with the United States. Properly addressing these considerations and identity data quality will enable all partners to utilize identity information to support their military objectives. While each PN retains ultimate authority for data sharing agreements consistent with its legal framework, CCPs can establish sharing recommendations, facilitate forums for developing these agreements, and suggest solutions that minimize partners' standards and systems differences.

Intentionally Blank

APPENDIX A
IDENTITY ACTIVITIES SUPPORT TO OPERATIONAL MISSIONS

1. Introduction

a. Identity activities support and enhance a significant amount of offensive, defensive, and stability activities. Identity activities play an especially critical role in any OE where there are dynamic populations of civilians, criminals, opportunists, facilitators, terrorists, and irregular forces. Within this complex environment, the ability to identify, characterize, and effectively manage the identities of enemies, adversaries, and persons of interest alike becomes essential to mission success. Whether conducting military engagement, security cooperation, crisis response, limited contingency operations or large-scale combat operations and campaigns, forces will conduct identity activities to achieve their mission objectives.

b. Below are several examples of typical mission sets that leverage identity activity capabilities to achieve military objectives. This list is not all inclusive, but demonstrates the value of identity activities across the competition continuum.

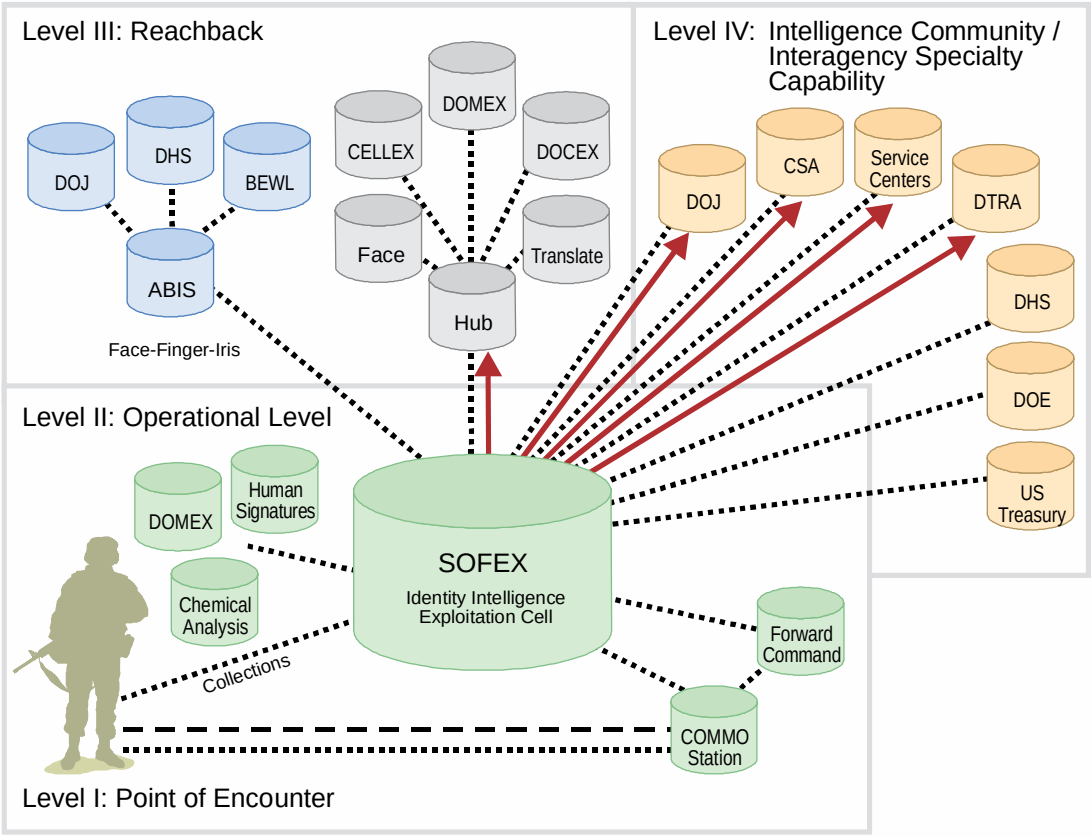
2. Support to Peer/Near Peer Information Collection

Support to information collection ranges from traditional counterintelligence and human intelligence information collection techniques threat assessment screening, encounter management activities, special reconnaissance and JIPOE. Peer/near peer collections facilitate development of population databases and intelligence holdings. The collection, processing, exploitation, and dissemination of this information can lead to better understanding of adversary or enemy patterns of activity, intent and capabilities.

a. Exploitation efforts in areas where adversaries or enemies are supporting indigenous forces that oppose US or PNs' supported governments or interests provide key understanding of training techniques and employment of capability previously unknown to intelligence analysts and operational planners. Accurate processing of human signatures, chemical analysis of materials, and DOMEX is possible at the tactical and operational level using trained officers and enlisted personnel using level 1 tactical and level 2 operational capabilities. Forward deployed civilian support at level 2 labs provides additional capability to support CCDR requirements. CONUS based level 3 reachback support by DOD components and other USG departments' and agencies' strategic lab capabilities supports further advanced exploitation, long term analysis, and storage of materials for future exploitation.

b. The ability to collect and properly process identity information is key to ensuring the IC has full discoverability of collected material and its subsequent exploitation. Flat architectures, similar to USSOCOM's SOFEX portal (see Figure A-1), provide quick

Special Operations Forces Exploitation Case Management and Data Transport Architecture



NOTE:
All information in SOFEX portal is available to anyone with NIPRNET or SIPRNET access. All lab results are posted in authoritative databases and SOFEX portal.

Legend

ABIS	Automated Biometrics Identification System
BEWL	biometric-enabled watchlist
CELLEX	cellular exploitation
COMMO	communications
CSA	combat support agency
DHS	Department of Homeland Security
DOCEX	document exploitation
DOE	Department of Energy
DOJ	Department of Justice
DOMEX	document and media exploitation
DTRA	Defense Threat Reduction Agency
FEDEX	Federal Express
NIPRNET	Non-classified Internet Protocol Router Network
SIPRNET	SECRET Internet Protocol Router Network
SOFEX	special operation forces exploitation
USSOCOM	United States Special Operations Command

SOFEX
radio
FEDEX tracker
USSOCOM
biometrics
forensics
DOMEX

Figure A-1. Special Operations Forces Exploitation Case Management and Data Transport Architecture

access to the CCMD's analytic efforts and IC reachback capabilities. All concerned leaders and analysts can view exploited material and its processing from level 1 collection and exploitation at the point of encounter to level 2 (in theater) exploitation at an EAC, DIA, DFSC, or Service lab. Exploitation architecture should also include a means for level 3 (strategic) to post results at the lowest classification possible.

c. Simultaneously, analysts from the collecting unit and their CCMD, DIA, and IC counterparts can begin to deliberate on the importance of the information collected and how it validates or changes existing doctrinal templates, threats and warnings, or priority information requirements. Additionally, counter-threat elements within DOD and the USG will have access to the information to devise counter-threat and risk mitigation measures to support US and PNs' information activities, planning, and strategic decision-making processes.

d. The ability to support special reconnaissance, post operation clearing actions, and rear area security presents a great demand on exploitation resources. The ability to deploy trained personnel to quickly and accurately conduct level 1 exploitation at the point of encounter speeds the ability to exploit the material at higher levels. Forward deployed level 2 capabilities provide a means to quickly transmit the exploited information to the supported commander and the IC for incorporation into planning, force protection measures, intelligence assessments, and decision making.

3. Alien Migrant Interdiction Operations

Alien migrant interdiction operations are as much humanitarian missions as they are law enforcement. The United States Coast Guard (USCG) is the lead agency for the enforcement of US immigration laws at sea. The USCG patrols and coordinates with a multitude of federal, state, and local agencies, as well as foreign nations, to interdict illegal migrants at sea. USCG personnel involved in law enforcement activities and operations may only collect biometrics as part of a nationally approved program, or when approved on a case-by-case basis by the USCG Assistant Commandant for Response Policy. Per business rules established through a DHS interagency agreement on the collection of biometrics at sea as part of the USCG undocumented migrant maritime interdiction program, collection of biometric data at sea in any geographic area is permitted from all migrants, regardless of nationality or diversion to protection pre-screening. Under these rules, collection on suspected smugglers, including US nationals or lawful permanent residents meeting certain criteria is also authorized. Aside from migrant interdiction operations, USCG personnel are also authorized to collect biometric data when there is reasonable suspicion of criminal activity, but only once the boarding team commences a criminal investigation. This collection is geographically limited to the Western Hemisphere Transit Zone and supports the safety of USCG personnel during maritime law enforcement operations and the positive identification of persons suspected of criminal activity.

a. Currently, the USCG conducts biometric screening on both migrants and those who smuggle them in the Mona Pass off the coasts of South Florida and Puerto Rico.

Biometric and biographical information is collected in an attempt to positively identify each individual.

b. This information is submitted through the Customs and Border Patrol National Targeting Center, then simultaneously screened against DOD's ABIS, FBI's NGI, and DHS IDENT. Only in DHS IDENT is this information retained for future identification. If there is a derogatory match within any database on the migrant(s) or smuggler(s), that information is sent to the appropriate sector command center.

c. Simultaneously, biographical information obtained from the migrant and/or smugglers is transmitted to the USCG maritime intelligence detachment to initiate development of an I2 report for each migrant. An established regional concurrence team provides a disposition for any matched or unmatched persons for follow-on action.

d. In some cases, the matched migrants are turned over to local border patrol authorities for processing and/or prosecution. Watch-listed and warranted individuals are turned over to local authorities for prosecution on outstanding offenses. All other persons onboard are repatriated in accordance with existing bilateral agreements as determined by a regional concurrence team established by the *South Florida Maritime Border Interagency Group Migrant Smuggling Prosecution Standing Operating Procedures*, or the *Caribbean Border Interagency Group Migrant Smuggling Prosecution Standing Operating Procedures*.

For more information on USCG collection of biometric data at sea, see Commandant of the Coast Guard Instruction (COMDTINST) Manual M16247.1, US Coast Guard Maritime Law Enforcement Manual. *For more information on USCG support to migrant interdiction operations, see NTTP 3-07.4M/COMDTINST M16247.4,* Maritime Counterdrug and Alien Migrant Interdiction Operations.

4. Department of Defense Installation Access and Entry Control Points

a. Identity activities are powerful force protection tools joint forces should employ identity capabilities in installation access and entry control point (ECP) missions for US-controlled facilities.

b. ECPs provide controlled access to specific areas, canalize traffic, or positively identify those who are passing through a given area. They are also frequently used to support other operations, to screen employees; control facility, warehouse, or storage access; and protect defense critical infrastructure. Identity activities support checkpoint operations by positively identifying those passing through the checkpoint. Biometrically enabled access processes, used in conjunction with a regular screening process at the ECP, protect our forces and those of our PNs by positively verifying individuals.

(1) Fully enroll all personnel who are authorized regular access to an installation and issue them a biometrically enabled access card. Regardless of past efforts, do not assume this has been done.

PERSONNEL SCREENING AND VETTING FOR INSTALLATION ACCESS

The new installation Commander at Kandahar Airbase has determined the need to fully enroll and verify the identity of all locally employed personnel (LEP) working on the installation. It is estimated this operation must support the screening of 1,600 personnel.

The local contract team checks the personal identification of each LEP and performs a full biometric enrollment. The security team checks each enrollment against the latest biometric-enabled watchlist before submitting it to the Department of Defense authoritative database for matching. Full biometric enrollments of individuals include fingerprints, iris images, facial images, plus biographical information and the contextual data related to the collection event. All enrollment information is retained for recurrent vetting purposes and to support future employment verification activities.

Various Sources

(2) Biometrically screen all personnel entering or leaving the base even if they possess an access card. A biometrics handheld collection device does this very quickly.

(3) Plan and establish checkpoints for verification.

(4) Canalize all traffic to checkpoints.

(5) Use overwatch to spot individuals trying to avoid checkpoints.

(6) Ensure up-to-date BEWL, for the unit's operational area, is uploaded to the handheld collection devices for verification.

(7) Plan for full electronic biometric transmission specification enrollments of suspect individuals.

5. Border Control/Ports of Entry/Maritime Interception/Checkpoints

a. Biometric identification and screening is extremely effective for managing and tracking cross-border movements. Checkpoints provide an effective means to stop the flow of foreign fighters and seal off the JFC's area of interest. Our enemies may find sanctuary across a border, but identity activities that include biometric screening makes the task of crossing a border an extraordinarily risky venture.

b. Identity activities immediately create complex terrain for the enemy by limiting the corridors they can use to access an operational area. Tracking personnel at ports of entry and border crossings produces a great wealth of information on their movements. Repeated crossings show a pattern of behavior that reveals potentially useful information, such as migration patterns and trafficking routes.

6. Support to Site Exploitation

a. Site exploitation operations involve highly trained team members who have specific duties during the operation but should also be cross-trained so they can accomplish the mission if something happens to a team member. Regardless of whether conducting a deliberate or hasty site exploitation, prior planning is the key to success. Information collected is used for a variety of future missions but two important aspects of site exploitation are to properly record and preserve the evidence for future prosecutions.

b. Exploitation (forensic, technical, and mechanical) of physical materials is accomplished through a combination of forward-deployed and reachback resources to support the commander's operational requirements. The exact mix of exploitation resources will depend on the threats identified by JIPOE, the JFC's mission, and the resources available from PNs. During irregular warfare, commanders are concerned with identifying the members of and systematically targeting the threat network, addressing threats to force protection, denying threats access to resources, and supporting the rule of law. Information derived from identity activity exploitation can provide specific information and actionable intelligence to address these concerns. Identity activity exploitation capabilities employ a wide array of enabling capabilities and resources, from forward-deployed experts to small cells or teams providing scientific or technical support, interagency or partner laboratories, and centers of excellence providing real time support via reachback. These exploitation capabilities can be employed individually to provide targeted support to distinct missions and/or functions, or together in a modular format under a common C2 construct.

(1) Site exploitation teams are specifically detailed and trained to conduct systematic search and discovery operations and properly identify, document, and preserve at the point of collection.

(2) EOD personnel have special training and equipment to render explosive ordnance safe, make intelligence reports on such ordnance, and supervise its safe removal. EOD personnel exploit an incident site, providing post-blast investigation expertise and site exploitation support, including a tactical characterization of the incident and a technical categorization of the device.

(3) Weapons intelligence teams are task organized teams that exploit a site of intelligence value by collecting exploitation-related materials, performing tactical questioning, collecting forensic materials, preserving and documenting DOMEX, providing in-depth documentation of the site, evaluating the effects of threat weapons systems, and preparing material for evacuation.

(4) When WMD or hazardous chemical precursors may be present, CBRN personnel can be detailed to supervise the site exploitation. CBRN personnel are trained to properly recognize, preserve, neutralize, and collect hazardous chemical, explosive, or drug-related materials. The CBRN personnel have an integrated EOD capability to mitigate CBRN threats. All site exploiters should be trained on WMD, hazmat, and precursor recognition.

(5) United States Navy surface combatants and Marine Corps units employ VBSS teams for detecting CBRN materials; collecting biometric and biographical information; conducting tactical questioning; and preserving and documenting captured enemy documents and media, including cell phones and contextual and electronic data for DOMEX. Marine Corps and Navy VBSS teams can be augmented by intelligence exploitation teams to facilitate human intelligence and tactical site exploitation activities. Where IEDs or explosive hazards are likely, EOD and combined explosives exploitation cell (CEXC) platoons can be assigned to support the VBSS missions.

(6) The United States Marine Corps and USSOCOM maintain deployable exploitation analysis centers to support forensic exploitation requirements around the globe. Each exploitation analysis center provides a forensic capability with the necessary equipment and trained personnel to execute select forensic exploitation activities in an expeditionary environment.

(7) The United States Army also maintains and deploys forensic exploitation teams (FXTs) staffed by civilian forensic scientists, who conduct confirmatory scientific testing when requested by a CCMD or JTF. FXTs provide an expeditionary forensic exploitation capability, including latent print examiners, DNA examiners, forensic chemists, firearms/tool mark examiners, electronic engineers, DOMEX personnel, and support personnel from a modular pool, task-organized to meet mission requirements. An FXT can also be deployed modularly with other Service exploitation capabilities. FXTs enable I2 and DOD law enforcement CRIMINT analysis and production at all echelons with exploitation results that meet International Organization for Standardization accreditation standards, although their primary customers are tactical and operational commanders.

(8) USSOCOM maintains deployable exploitation analysis centers (and regional exploitation centers) to support exploitation requirements around the globe.

(9) CEXCs are a Naval Surface Warfare Center, EOD Technology Division deployable capability that is scalable in skills and size, enabling them to be tailored to meet the commander's requirements, including incorporation of multinational and interagency partners. CEXC personnel are trained and equipped to conduct technical intelligence operations involving recovered improvised weapons systems and provide near-real-time intelligence on their construction and employment. CEXC processes support identity activities by identifying IED trends and bomb makers, providing insights into enemy tactics, and assisting in the development of defensive and offensive C-IED and other improvised weapons defeat measures. CEXC supports I2 and DOD law enforcement CRIMINT analysis and production at all echelons, although its primary customers are tactical and operational commanders.

(10) The FBI's TEDAC serves as the single interagency organization to receive, fully analyze, exploit, and provide a repository for all terrorist IEDs of interest to the United States. The TEDAC coordinates efforts of the entire government, including law enforcement, intelligence, and military, to gather and share intelligence about these devices. TEDAC provides direct support to broader USG efforts to prevent and mitigate

IED attacks by performing advanced exploitation of IEDs through physical examination, resulting in scientific and technical information and valuable intelligence. Through its integration of intelligence resources, the TEDAC also provides expeditious reporting of raw and finished intelligence to intelligence and law enforcement partners about device attributes and terrorist TTP to enhance knowledge and understanding of current and future threats.

DELIBERATE SITE EXPLOITATION

Detection. Recent human intelligence (HUMINT) reporting has indicated a mid-level terrorist leader frequents the home of the village elder following Friday prayer. This home has been previously reported to multinational forces as a terrorist safe house. Further reporting indicates he meets with a local terrorist cell leader here. The dossier on the village elder indicates he is employed as a metal fabricator and has eight family members who live at this home.

Locate/Identify. Imagery from an unmanned aerial system (UAS) and from walking patrols of the village elder's home are collected and analyzed. Images of persons detected are matched against known locals who have provided identification as well as been previously biometrically enrolled. Facial matching indicates there is a high possibility that two local farmers also attend these meetings. The UAS reveals the home is a three building compound surrounded by an 8-foot wall. A white truck arrived first carrying three military-aged males (MAMs) with assault rifles. A small blue sedan arrives shortly after Friday prayer with two MAMs, both entered the home. UAS imagery indicates that the village elder's family has left the main house and gone to the rear quarters. The meeting lasts for one hour and ten minutes. A forensic collector with a walking patrol arrived two hours later and recovers a water bottle and three cigarette butts from the vicinity where the white truck had parked. Latent fingerprints from the water bottle and DNA [deoxyribonucleic acid] from the cigarette butts match a biometric enrollment from two former detainees who were released six months ago. They were suspected low level terrorists who were detained on weapon charges.

Target Nomination. A target folder is developed on the house, and the persons of interest: the village elder, the two unknown persons who entered the home, two local farmers, the two former detainees, and the unknown person with the white truck. Biometric dossiers are added to the targeting folder.

Preparation. All of the developed biometric dossiers are uploaded into two portable handheld biometric collection devices along with the current biometric watchlist and biometric dossiers of the villagers. The

first device will be carried by the initial assault team. The second device will be carried by the follow-on security force. To minimize risk to civilians, it is determined to strike the house five minutes after the arrival of the blue sedan giving time for the family members to exit the main building. The threat security force in the white truck along with the house would be hit simultaneously. All persons in and around the house will be biometrically enrolled and matched before being released.

Execution. The initial assault resulted in the capture of nine MAMs inside the house and the killing of two MAMs at the white truck. All were asked to show identification documents as well as enrolled/matched with biometric collection devices. Five of the eleven were previously enrolled aiding initial tactical questioning. The security team arrives minutes after the compound is secure and occupants are segregated. The multifunctional team begins gathering documents and computers, the HUMINT collectors begin the initial interrogation.

Imagery of the compound and all known pertinent data has been given to the planners for use in planning a successful site exploitation mission. All historic and habitual activities and social relationships are studied by the team to try and forecast all situations that might be present upon arrival of the team. A targeting mission has been planned by special operations forces to capture or kill insurgent members if encountered on this location. The site exploitation team has been put on alert that as soon as the initial mission has concluded the team will be transported to the location by helicopter to exploit any and all useful artifacts or paperwork for future intelligence value or prosecution efforts.

Various Sources

HASTY SITE EXPLOITATION

The site exploitation team, currently deployed to forward operating base Jasmin in the Helmand Province, has been training on proper procedures for collecting data in various scenarios. Several scenarios have been developed by the operations staff that seem to categorize most missions that the site exploitation team would need to be able to accomplish. One mission involves possible improvised explosive device (IED) makers being targeted and when the team arrives they find various devices used for making IEDs along with several military-aged males who appear to be associated but not previously targeted by allied forces. Other scenarios depict failed targeting attempts because the level 1 target sought was not at the location. Evidence at the scene however led the leadership to deploy the site exploitation team because a very high-level al Qa'ida leader was presumed to frequent the residence.

The team is currently being deployed to an embassy where multiple fatalities have occurred and one of those was a very high ranking member of the Afghan government. Explosive ordinance disposal members have cleared the area for the site exploitation team. Team members are hurried to the location where they begin sifting through the wreckage and litter. Members find pieces of the bomb that was reportedly triggered by a cellular phone and believed to be delivered by a suicidal insurgent. Shards from the bomb are carefully tagged, recorded, and transported to a laboratory located in the area. Chain-of-custody is carefully adhered to and, if fingerprints are found on the shards, they will be sent to various databases to determine whether a match can be made with an already-collected fingerprint. Once the fingerprints are matched and a high-value individual is added to the biometrics-enabled watchlist, soldiers can focus on finding and prosecuting the individual responsible for murder and terroristic activities.

Various Sources

7. Support to Partner Nations' Census Operations

The employment of biometric technologies and robust information systems makes large scale biometric supported census operations feasible and practical in support of PNs. Census planning considerations:

a. Locate and identify every resident.

b. Visit and record every house and business.

c. At a minimum, when authorized to do so, fully biometrically enroll all military-age males with full sets of fingerprints, full face photo, iris images, and names, including all variants.

d. Record biographical data, including addresses, occupation, tribal name, and military grid reference of enrollment.

8. Support to Civil-Military Operations

a. Identity activities serve as invaluable tools for establishing or reestablishing the legitimacy of local authorities in activities that build or restore the PN's capability and capacity. The focus of such operations is to improve PN government capability and capacity to provide public services to its population, thereby enhancing legitimacy of the PN government, enhancing force protection, and accomplishing the JFC's objectives. Support to CMO should emphasize long-term developmental programs that are sustainable by the HN. Use of biometrics-enabled identity management tools to manage refugee movement and relocation efforts can expedite such operations while increasing security. A unit's ability to leverage identity tools results in the means to rapidly reunite separated families. Accurately identifying families receiving aid (e.g., medical care, food, water, material, jobs) through the use of biometric signatures, controls distribution and helps to eliminate waste and black marketeering. Small units may frequently find themselves tasked to conduct or support CMO before, during, and after combat operations.

b. CMO planning considerations may include:

(1) Identify relevant actors in the OE.

(2) Plan for implementation of population control measures.

(3) In conjunction with the assigned legal advisor, ensure that biometric enrollments do not violate any international laws or policies.

9. Support to Cordon Operations

a. To find selected personnel or material, a unit will typically conduct a cordon and search or cordon and knock operation. There are two primary elements in a cordon and search operation: the cordon element and the search element. Both of those elements have requirements for the collection of identity information. The search team may use several approaches to the search itself, including central assembly and restriction to quarters or control of the heads of households. In each of these approaches, biometrics can be used effectively. The cordon element can also set up check points in which biometric collection devices are used to screen individuals seeking to enter or leave the cordon area.

b. Cordon operations planning considerations.

(1) Plan for collecting identity data to include biometrics in the operation order and/or fragmentary order.

(2) Plan to conduct biometric enrollments and screening.

(3) Ensure current watchlists and local alerts are loaded before mission execution.

(4) Ensure unit and/or patrol with handheld collection devices has taken enough extra charged batteries for completion of the mission.

(5) Use biometric handheld collection devices at checkpoints in the cordon to canalize traffic.

(6) Plan for positive or negative identification of personnel.

(7) Incorporate identity data into debriefs.

(8) Enroll everyone, to include all wounded in action and killed in action.

(9) Plan for forensic data collection, to include latent fingerprints from materials, documents, and media (e.g., pocket litter, found documents, found computers and cell phones).

10. Support to Counterinsurgency

a. Identifying the population in a particular area is essential to effective counterinsurgency operations. A unit needs to know who lives where, who does what, who belongs, and who does not in their operational area. While the actual term may be problematic, population management efforts are often seen as supportive of the local government, particularly if accompanied with a program that provides badges to authorized personnel which highlights the government's presence in an area. Local and tribal leaders, clan heads, and provincial governments use identity data to secure their populace against outsiders who arrive for the purpose of intimidation or other negative activities. Simply knowing who belongs in a village or area automatically spotlights those who do not. These operations also lend authority to local leadership by helping them keep unwanted individuals out of their areas and giving them the means to effectively protect their own people.

b. Every person who lives within an operational area should be identified and fully biometrically enrolled with facial photos, iris images, and fingerprints of all ten fingers (if present); along with their biographical data to include name, place of birth, scars, marks, tattoos, and other identifying information. This identity information should be coupled with other biographic data, such as where they live, what they do, and to which tribe, clan, village or town they belong. In this manner, a unit will more easily identify outsiders or newcomers. Identity information is also useful in the transfer of authority to another unit. A unit inheriting a current census becomes much more effective in a much shorter timeframe. Population management actions also have the effect of building good relationships and rapport, since the crafted message is that the census is intended to protect them from the influence of outsiders and will give them a chance to more easily identify troublemakers in their midst. Population management operations offer excellent opportunities to locate and identify every resident and to track persons of interest. Unusual travel patterns of individuals may indicate unusual activities.

c. Counterinsurgency planning considerations.

(1) Visit and record every house and business.

(2) At a minimum, fully biometrically enroll all military age males with full sets of fingerprints, full face photos, iris images, names, and all variants.

(3) Create an enrollment event for future data mining.

(4) Ensure enrollments are conducted and sent into DOD ABIS, the authoritative biometrics database for DOD.

(5) Collect and assess CMO data.

(6) Identify local leaders and use them to assist in identifying the populace.

(7) Use a badge system to identify local leaders and key personnel.

(8) Report potential human intelligence sources to the local J-2.

(9) Designate indigenous forces as the lead at every possible opportunity for identity activities.

(10) Intelligence sections should designate specific named areas of interest to support identity collection activities on specified persons of interest.

11. Support to Detainee Operations

a. During military operations, joint forces must be prepared to detain a wide array of individuals. Some of these detained persons (hereafter referred to as detainees) will result from international armed conflict and will fall into the conventional category of POW. Other categories of detainees, however, will likely result from military operations that are not typically considered international armed conflict (e.g., FHA, peace operations, noncombatant evacuation operations) or may result from their particular conduct or status of the detainee (i.e., belligerent, retained personnel, civilian internee).

b. Personnel detained for any reason should be completely biometrically enrolled as quickly as possible following initial detention. Personnel detained for one reason may be found to have several other reasons for a unit to continue detaining them. Biometric matches may also provide the linkage between an individual and an event that may provide the justification for civilian trial and internment. At a minimum, it provides a tracking tool for every individual detained for whatever reason across the operational area. When authorized, it also provides a highly effective intelligence interrogation or detainee debriefing tool in that a trained and certified interrogator or debriefer has more positive knowledge of a subject's movements.

c. The collection of identity data provides specific information that may be of great use in interrogation. Identity data may also identify detainees who are not on the BEWL. Some of these detainees may be released. Depending upon available information, and/or intelligence, detainees may also be nominated to the BEWL if it is warranted. When

integrated into the overall detainee tracking and management process, biometric data verifies and supports the decision to release or transfer an individual. Biometric data enables the tracking and management of detainees within detention facilities to include departure and arrival times at various internal detention facility services. Commanders must ensure unit procedures do not conflict with the law of war, US law, DOD policy, and if applicable, HN laws or other regional and local policies and agreements.

d. Identity activities enhance a unit's ability to:

(1) Positively identify detainees.

(2) Confirm involvement in illegal or criminal activities.

(3) Track details of interactions with detainees throughout the detention process to include release (prevent the release of the wrong person).

(4) Avoid identification mismatches due to changing and/or multiple versions of names.

(5) Individualizes personnel, i.e., regardless of how many individuals with the same name there are in the world, each one has a unique set of biometrics that differentiates them.

(6) Prepare for effective interrogation by checking the BEWL and other activities.

(7) Assist HN prosecution of individuals through identity data matches.

For more information, refer to JP 3-63, Detainee Operations, and DODD 2310.01E, The Department of Defense Detainee Program.

12. Support to Foreign Internal Defense

Joint forces regularly train the forces of PNs and regional allies. US forces are dependent on the PN to verify that those receiving our training and the benefit of our expertise are, in fact, the individuals that the PN (and the United States) want to train, and not adversaries. By verifying the identities of individuals receiving the training (especially through the use of biometrics), and vet, the individual trained, we reduce the likelihood of training our present or future enemies. Advising the PN on the use of identity activities for such verification provides yet another means of contact with PN authorities and an avenue for further education on the usefulness of identity capabilities (such as biometrics). Using identity data to vet those personnel receiving training assists US forces to identify those who should not receive training. It also identifies those personnel whose documented conduct might be a cause for concern.

EXAMPLE OF IDENTITY ACTIVITY SUPPORT

United States (US) and multinational forces are supporting a foreign state's rebuilding process, which is being undermined by smuggling into the state. The host government has only allowed US forces to use collected biometric data within the host nation. Therefore, all biometric operations are conducted using local un-trusted sources (i.e., the data is not stored in the trusted Department of Defense authoritative database).

In accordance with standard operating procedures, a truck driver provides his identity data and biometric samples to the border police at a remote international border crossing supported by US military personnel. The biometric samples and contextual information are transmitted to the local un-trusted source and subsequently compared to locally stored biometric files. The truck driver's biometric data does not match any file at the local un-trusted source and a negative response is provided back to the border police. The truck driver also is checked against local and national criminal records. The border police review the driver's provided identification, match result, associated information and other available situational information and clear the truck driver to continue. The biometric file is enrolled and stored at the local un-trusted source, as well as shared with US forces, multinational partners, and nongovernmental organizations operating within the host nation.

Several months later, the host nation's national police, supported by a US Government department or agency, conduct a raid on a drug smuggler's safe house and seize numerous documents and other evidence. Forensically collected latent fingerprints are compared to the local database. A match is made between the samples collected during the raid and the truck driver's previous biometric file on file. An analysis of the raid, as well as additional associated information, is completed and the truck driver's non-biometric reference information is updated with these new samples, identified for future matches, and shared with all local sources within the host nation.

Several days later, the truck driver attempts to cross at a different border checkpoint. He submits his individual identification and a biometric sample for verification. The sample is compared against the truck driver's biometric sample on file, which alerts the border police to the data stored at the local un-trusted source. The truck driver is detained for questioning and his biometric file is updated with the newly collected biometric sample and contextual data.

Various Sources

13. Support to Foreign Humanitarian Assistance

a. Identity data can play a critical role in FHA operations even if the HN does not have an automated identity data collection enrollment protocol or database. Humanitarian assistance and other logistic support can be provided for a number of reasons, both natural and man-made. The distribution of such aid, however, should be carefully controlled to ensure everyone gets their proper allotment without anyone being able to stockpile or hoard relief supplies. A biometrics signature provides a way to track who has or has not received aid. The employment of identity activities both ensures there will be sufficient supplies of aid and that no one unfairly benefits from FHA operations to the detriment of the population that requires the aid (and, of course, ensures we do not inadvertently deliver aid to criminal elements and other adversaries). It should also prevent availability of relief supplies on the black market, which is inimical to both our interests and those of the HN. Biometrics can be used to enroll all recipients of humanitarian assistance to ensure there is no "double dipping" into humanitarian assistance resources. Biometrics as a receipt verification protocol can dramatically limit black marketeering or other fraudulent receipt of relief supplies. Tracking those to whom assistance has been provided is easily verified through fingerprints or iris images. In the same manner that humanitarian assistance may be controlled by the use of biometrics to prevent profiteering, medical and dental assistance benefits likewise from the same function.

b. FHA planning considerations.

(1) Biometrically enroll all recipients of humanitarian assistance to ensure no double dipping into humanitarian assistance resources.

(2) Using DNA testing, reunite families after a disaster.

(3) Ensure we do not provide aid to anyone on the BEWL or who has had a latent print recovered from a site of anti-MNF activities.

DISASTER RELIEF

The US Government is responding to a request from a nation that has experienced a catastrophic disaster. The disaster has created the immediate need to locate, rescue, and manage the affected population. The host government approves the multinational response force to collect biometric samples from the civilian population to assist with disaster relief efforts with the stipulation that the biometric information only is used to identify individuals located and rescued and to manage the flow of casualties and the displaced population; and the biometric information not be removed from the host nation.

Biometric data is collected as the affected individuals are rescued, treated, or entered into the refugee management process. Joint force personnel utilize the collected biometric files stored in the local un-trusted source as the reference set against which subsequent matches are made. As personnel are placed aboard transportation, provided medical and/or dental care or basic services at a disaster relief site, the individuals' biometrics are the "tokens" that authorize their access. In each instance, once the biometric file is matched, the identity is referenced against repositories of non- biometric information (e.g., camp rosters, medical records, records of service provided, transportation logs) to enable better management of services provided and needs of the population. This data and the collected biometrics are shared with the host nation and multinational partners to assist in integrating their relief efforts with those of United States forces. The host nation also compares the collected information with whatever repositories of non-biometric data may have survived the disaster (e.g., tax records, census data, voting records, individual identification records) to assist in the speedy location and reunion of families. At the request of relief organizations, the national government shares the identity data and identification results with nongovernmental organizations and neighboring nations affected by the refugee flow.

Various Sources

FOREIGN HUMANITARIAN ASSISTANCE—RELIEF MISSION

The United States (US) military is responding as part of an international disaster relief effort. Thousands of injured are being treated and awaiting further treatment as soon as field medical hospitals are assembled and operational. All individuals who receive medical attention within the disaster area are immediately enrolled in a Department of Defense biometric local un-trusted source that has been established for management of the refugees. All treatment records are linked to their respective biometric files. Many of the injured, after being initially treated, voluntarily relocate within the disaster area. This movement is making it difficult for medical personnel to efficiently provide medical services or track patients for follow-up treatment.

US Navy corpsmen are performing triage for refugees arriving by buses at one of the newly established US field hospitals. The corpsmen collect biometric samples from each refugee for identification purposes as part of the initial medical assessment process. The biometric files are then sent for matching against the local un-trusted source to assist with the identification of the individual and retrieve any available treatment history.

A refugee who cannot be matched against the local un-trusted source is enrolled as a new biometric file. All subsequent medical treatment will later be linked to that file. When a refugee is positively matched against the local un-trusted source, links to his medical history are accessed and his prior treatment records are retrieved. Subsequent treatment is updated in the refugee's medical record so that information can be accessed by others again in the future through utilizing the established net-centric links between the non-biometric repository (medical files), his identification documents, and his biometric file. The corpsman uses these records to aid in triage.

Various Sources

FOREIGN HUMANITARIAN ASSISTANCE—SECURITY MISSION

The United States (US) and multinational partners operate from several dozen military bases in an allied nation and contract locally for a wide range of services, such as: vehicle rental and maintenance, civil construction, provisioning of food and water, and waste removal. Identity data, to include biometrics data, are collected to support a wide range of activities, from base access to monitoring all contracting activities. All biometric data are matched against the local trusted source and repositories of associated information for the purposes of vetting. All samples reveal a negative match and are enrolled in the local-trusted source and further transmitted to the authoritative source.

A contracting officer encounters a dishonest local contractor who is awarded contracts and receives partial payment but never finishes the work, essentially disappearing with the money. This associated information is reported to the intelligence directorate contractor vetting cell which analyzes with relevant identity and biometric data. This analysis is transmitted to the authoritative source, the individual's biometric file is identified, and repositories of associated information are updated to include putting the vendor on the "do not contract with" list, thus barring the vendor from receiving future contracts. This information is then shared with local-trusted sources and other interested parties.

The dishonest local contractor relocates to another region and applies for new US and multinational force contracts using a different company name and false personal data. Because the personnel identification requirement was in the contract, his identification documents and collected biometric sample positively match revealing the associated information indicating his previous activities and status. As a result, the dishonest contractor's bids are eliminated. The dishonest contractor's identification and biometric files are updated with the newly collected identity data, and the attempt is shared with all appropriate authorities.

A newly arrived disbursing officer is ordered into the local community to pay a contractor for recently completed work. This officer has never met the local national to whom he is to pay a large sum of cash. Following the directions provided by a local interpreter, the disbursing officer arrives at what he believes is the office of the intended contractor. Unbeknownst to the disbursing officer, he has arrived at a fake contractor's office. As a condition of payment the supposed contractor provides his biometric information. A field match test reveals the presented biometric samples do not match the biometric file of the individual identified in the contract. The disbursing officer refuses to pay despite the local interpreter's and contractor's insistence.

Upon returning to base the disbursing officer provides the collected biometric information and his incident report to the provost marshal for investigation with the local police. The local interpreter is immediately detained on-base for questioning. The fraudulent contractor's biometric

file is enrolled and stored within the local-trusted database, transmitted to the authoritative Department of Defense database, and shared with interested parties. Upon conclusion of the investigation, the provost marshal concludes that the contractor is a fraud. US military contracting offices operating within the region as well as the host nation update their respective repositories with this information.

Various Sources

14. Medical and Dental Care

a. In the same manner that FHA may be supported through the use of identity activities to prevent profiteering, so too medical and dental assistance lends itself to the same type of control. Collecting identity data can help prevent black marketeering of medical and dental supplies and double dipping into such aid through the use of identity vetting and biometric signatures to sign for the supplies. However, with medical assistance, it can have an even more positive impact by ensuring someone does not receive the same inoculation twice or gets more medication than they are due. Many people in rural areas do not understand why the medications they receive work so well and often have the philosophy, "If some is good, more is better." There is also the potential for "doctor shopping", whereby one patient sees multiple doctors to get extra medication (especially) narcotics that will be sold later.

b. Identity and biometric data enables positive control of the distribution of medical and dental assistance and ensures that no one receives more services and supplies than they should. US forces use biometric data, as well, for the tracking of records and care of its own forces. Medical aid is often well received regardless of politics. US aid providers should explain the need to create a record for adult individuals as part of the medical services. Handheld biometric collection devices blend in well in a medical environment especially since they measure physical traits. Medical civil action project and dental civil action project missions already incorporate cultural considerations and gender issues and provide a non-hostile collection atmosphere superior to a combat patrol or even a key leader engagement. Populations may then see identity data and biometric information collection as benign and associate its use with positive results.

c. Medical and dental care planning considerations.

(1) Biometrically enroll all recipients of medical and dental assistance to ensure no double dipping into medical and dental resources.

(2) Medical and dental care is available to all; however, some may receive it while en route to or in a detention facility.

(3) Track personnel throughout the medical care system, in evacuation channels or in hospitals.

(4) Visits to local hospitals and clinics can also be a great way to screen the local populace and increase enrollments into a database.

15. Personnel Screening and Vetting

a. US forces use a number of locally hired personnel in deployed areas for a variety of reasons. Local hires are essential to the effective operation of forward operating bases and can be found on virtually every installation operated by US forces. The use of identity data collection (to include biometric data) enables the screening and vetting of those locally employed personnel. This includes the vetting of local security forces that receive training by the United States to ensure they are not members or supporters of an insurgency, criminal elements, or other adversaries. The vetting of local leaders in deployed areas, especially during stabilize and enable civil authority phases, assures the populace that their leaders are not adversaries or criminal.

b. Planning considerations for personnel screening and vetting.

(1) Biometrically enroll all local nationals and third-country nationals directly accompanying the force, requiring access to a military controlled facility, or working on a USG-funded project.

(2) Biometrically enroll all local national company representatives who will receive direct USG payments and selected management personnel as deemed necessary.

(3) Biometrically enroll all local personnel receiving military training.

(4) Periodically verify the identities of the workforce.

(5) Coordinate with joint force headquarters OCS integration cell and supporting contracting office to ensure contracts require biometrics validation to receive payment.

16. Support to Populace and Resources Control

a. DOD support to various operations may require managing cross-boundary movement of HN civilians or managing aid and support distribution. These tasks can be streamlined and monitored through the implementation of identity screenings at various control points. Populace and resources control efforts are often seen as supportive of the local government, particularly if accompanied with a badge and/or a credentialing program that highlights the government's presence in an area.

b. Planning considerations for populace and resources control.

(1) Plan for identity data collection in the operation order/fragmentary orders.

(2) Plan for full biometrics enrollments.

(3) Plan, and establish, checkpoints for identity verification.

The Task Force Raider civil affairs team will oversee the contracting of locally based companies to construct a new school in Sarpuzen village, Dand District, Kandahar Province. The civil affairs team will vet all local national personnel to insure they are not associated with the Taliban or criminal activity. The civil affairs team has a 28-member construction team plus four company management personnel biometrically enrolled at Camp Nathan Smith.

The screening team will have biometric handheld collection devices with an updated Afghan biometrics-enabled watchlist (BEWL). Due to limited Internet availability and Nonclassified Internet Protocol Router Network bandwidth, biometric data submissions will utilize the SECRET Internet Protocol Router Network. The screening team must determine if any of the host nation's personnel are matched against the BEWL and must know if these individuals' biometrically match against any existing automated biometric identification system records or unsolved latent fingerprints that indicate insurgent or criminal activity.

Various Sources

(4) Ensure current biometrics watchlists are loaded before the mission.

(5) Plan for all electronic biometric transmission specification submissions to be sent to the DOD authoritative repository.

(6) Ensure authorized personnel receive badges and/or credentials after vetting their identification.

(7) Establish a village database to effectively assess individual access and placement.

17. Support to Targeting

a. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. These targeting actions imply both lethal and nonlethal effects. Successful high-value individual (HVI) targeting operations require identity activities data exploitation and other multidisciplined intelligence. Commanders must synchronize intelligence, maneuver elements (to include SOF), fire support systems, and other units as necessary to engage the correct HVI target at the correct time. Accurate identification and attribution is crucial when targeting individuals hidden amongst the population.

b. Identifying the specific HVI from the rest of the populace is crucial. Identity activities that include biometrics, forensics, exploitation, and multidisciplined intelligence and operational enablers enhance the ability of the commander to conduct rapid, successful targeting operations, and assist in determining what systems will be required to complete the operation.

Due to numerous improvised explosive device attacks along Highway 1 and several caches discovered, 2nd Battalion (BN)/Task Force (TF) Raider will conduct a population management mission to identify and manage the population of Pir-E-Paymal village, Arghandab district, Kandahar province.

Every adult or adolescent male who lives within the village (population of 1,200) is identified. Additionally, they are fully biometrically enrolled with facial photos, iris images, and all ten fingerprints (if present). This information is coupled with good biographical (name, notations of scars, marks and tattoos, where they live, what they do, and to which tribe or clan they belong) and contextual data (such as the context of the encounter). In this manner, a unit can easily identify outsiders or newcomers.

2nd BN has biometric handheld collection devices and will require a modified Afghanistan biometric-enabled watchlist (level 1 and 2 for Afghanistan plus all other levels for Kandahar Province) and they will utilize tactical radio communications with TF Raider headquarters in Kandahar City. 2nd BN also wants to submit all their biometric enrollments to the Department of Defense authoritative database to complete the identification process for the village and require a match.

Various Sources

c. Commanders follow a targeting process to provide an agile force with enough accurate and timely information to interdict, kill, capture, recover, observe, engage or substitute personnel, materiel or information. Identity activities support this process as part of a multidisciplinary effort. Targeting methodology facilitates identity- focused targeting and the full capability of technical exploitation to be realized and applied. Identity activities provide specific targeting requirements that refine the actions to be completed when engaging HVIs.

d. Planning considerations for targeting.

(1) Plan for identity activity data collection in the operation order and/or fragmentary order.

(2) Plan for full biometrics enrollments and verification process.

(3) Ensure current biometrics watchlists are loaded before the mission.

(4) Use biometrics to verify target(s).

(5) Identify other potential target(s).

18. Support to Stability Activities

a. Identity activities enable numerous missions related to stability activities, including but not limited to enforcement of sanctions; counter piracy operations; counterproliferation operations; highly accurate human environment mapping; preventing human trafficking; effective administration of FHA; and prevention of black marketeering and diversion of supplies for hoarding through the use of positive identity data and biometric signatures to sign for relief supplies. Identity activity data enables a commander to empower his counterparts in the national security forces by providing positive identification and vetting of their forces. This enables a commander to ensure that his forces have not been infiltrated by the enemy and adds to the legitimacy of his forces by increasing confidence among the populace that they are truly national forces and not personnel masquerading as such. Identity activity capabilities also assist in the identification of criminal elements, insurgents, and other adversaries.

b. Support to stabilization planning considerations.

(1) Biometrically enroll, screen, and vet all local police, army, and security forces.

(2) Use identity activities (to include biometric data collection) as a means to work more closely with HN forces (help your counterparts to be successful by culling undesirables from their ranks).

(3) Inform commanders about the true background of some of their personnel (an HN policeman might prove less effective as a policeman if he has previously been banned from an American base for stealing or is identified as belonging to an adversarial group that intends to kill or injure PN personnel within the HN police or armed forces).

While on patrol, a squad of Marines detects an improvised explosive device (IED). Explosive ordnance disposal technicians render the device safe, a forensics team manages to collect latent fingerprints and deoxyribonucleic acid (DNA) samples, and the IED components are sent to a forward forensic facility for more analysis.

The latent fingerprints are formatted into a standardized electronic file, compared to samples on file and stored locally. There is no match at the local-trusted database source and the data is enrolled into a biometric file for further processing and comparison. Both the electronic fingerprint file and DNA samples are transmitted to their respective authoritative databases for further comparison. Acknowledgement of receipt is transmitted back to the local source. Matching at the authoritative data repositories does not yield a DNA match and the sample is stored for further comparison. The biometric samples are shared with partner nations (PNs), revealing a fingerprint match to a suspected bomb maker. Based on this identification, the PN provides a facial photograph of the

suspected bomb maker as well as other intelligence derived from captured documents and other sources.

Analysis of the identity data, biometrics, contextual, and associated information indicates that the suspect's last known location is outside of the joint area of operations in a third country providing sanctuary. This analysis, as well as the photograph provided by multinational partners, is sent to the Department of Defense biometric authoritative repository to update the biometric file. An alert (prompt) containing links to information located in non-biometric reference data is disseminated to tactical users to facilitate future data comparisons on their local biometrics systems should they encounter the individual.

A series of raids on suspected insurgent locations provides more identity data and biometric samples that are matched to the suspected bomb maker. This match information, the biometric files, and the associated information from the previous analysis that led to his being tied to the IED incidents are shared with interested parties for further analysis. Analysis of associated information indicates that the suspected bomb maker is moving within the area of responsibility and provides locations he will likely move to. Cameras are positioned around those locations (now an identity named area of interest) and provide photographs that identify the suspected bomb maker using facial recognition. Once the suspected bomb maker is located, a tactical unit conducts a raid to apprehend him.

The raid force encounters six men at the site, all with authentic-looking local government identification in their possession. Pictures of the bomb maker provided to the raid force are outdated and do not closely resemble any individual at the raid site. However, there is a biometric fingerprint match to the suspected bomb maker. Analysis of that biometric match result and associated information from the previous analysis that tied him to the IED incident enable the raid force leader to decide to detain the individual. The other men are released after collecting their biometric samples and comparing them against available repositories to determine if they had been encountered previously. All collected samples and contextual information are updated in their respective biometric files and annotated to reflect that the raid force encountered them in the company of a known bomb maker. Other information found at the scene is also collected by the raid force and subsequently stored in a repository of associated information for use in later analysis.

Various Sources

c. Identity activities enable commanders to control and manage the distribution of property to HN personnel. Requirement of a biometric signature, such as fingerprints, from those receiving supplies of any sort prevent those same supplies from diversion, hoarding, and resale. While adding to the overall identity databases, it also ensures that payments are made to the correct person by verifying that person's identity. The US forces frequently use locally employed personnel in the conduct of logistic and transportation operations. The biometric enrollment and vetting of locally employed personnel, as required by the Federal Information Processing Standard Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, mitigates the hiring of adversaries and criminal elements.

19. Support to Countering Weapons of Mass Destruction

Identity activities can be valuable in countering WMD. International cooperation on precursors and essential components, supplemented by identity activities data, can prevent the proliferation of such weapons, identifying personnel associated with various storage sites and involved in their trafficking. Personnel apprehended on site with WMD can be positively linked to the weapon by matching latent fingerprints and DNA found on key components or in key locations to the biometric records of personnel, separating innocent personnel from those who had intimate access to the weapons themselves. Forensic exploitation of WMD can also provide valuable information as to the source of supply of critical components and yield detailed information about supply chains, providing more effective response and interdiction possibilities.

20. Support to Chemical, Biological, Radiological, and Nuclear Response

Biometrics enables the JFC to closely control access to CBRN-affected areas and to physically control access to residents and authorized personnel only. Simple iris image technology can give the commander the ability to decide who can or cannot enter a particular area. In a CBRN incident, this ability offers clear operational advantages. By scanning the irises of all legal residents and authorized personnel and placing them in a simple database, commanders create the ability to control access to any cordoned area. Forensic processing of the scene is simpler, containment is easier, and future medical treatment, if needed, can go to those actually affected, focusing resources and reducing incidents of attempted medical fraud.

21. Support to Counter Threat Finance

Forensic techniques are key factors when it comes to tracking financial transactions and financial activities. Criminal and insurgent activities are dependent on adequate funding. The forensic exploitation of digital media, computer hard drives, cell phone histories, and subscriber identity module cards provides the tools needed to track the history of financial transactions from the end user back to the source, enabling US forces to identify both personnel and opportunities to interdict funding of illicit activities. Using forensic techniques to trace financial records and identify financiers also enables the JFC to reinforce the rule of law and individual sovereignty of PNs. The use of identity data is also used to track finance records for friendly forces.

APPENDIX B
ASSESSMENT INDICATORS FOR IDENTITY ACTIVITIES

1. This appendix provides examples of the objectives, effects, and indicators for identity activities. While not all inclusive, it does provide a start point for operation planners. The ultimate use of these measures, as well as additions to, deletions from, and other changes to them is up to the JFC and subordinate commanders.

2. The identity activities assessment indicators listed in the figures follow the guidance provided by JP 5-0, *Joint Planning*. Identity activities feed the operational assessment process and, therefore, must identify the indicators necessary for identity activity planning and execution throughout the competition continuum.

3. Figure B-1 should be considered an umbrella identity activity assessment indicator figure. Additional mission-specific identity activity considerations and indicators are provided in Figures B-2 through B-32.

Example: Objective, Effects, and Indicators for Identity Information and Data (to Include Biometrics, Forensics, and Other Exploitation)				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to enhance missions throughout the competition continuum.	1. Identity activities are planned for, inserted into operation plans and operation orders, and executed.	1. Ensure bilateral agreements are in place between the US and partners nations (PNs) in order for US forces to collect, store, and share identity (to include biometrics, forensics, and other exploitation) information and data. Include identity activities in theater campaign plans/theater security cooperation planning and that they do not violate any international law or policies (to include the rules of engagement and applicable standard operating procedures in dealing with any local populace).	Qualitative/ Objective	Prior to conducting identity activities within the operational area.
		2. Use J-2/G-2 (intelligence planning) and J-3/G-3 (operation planning) to plan for, execute, and assess identity activities (identification and forensic data) that will gather and secure evidence.	Qualitative/ Objective	Planning, execution, and assessment of identity activities as well as collection of forensics and/or other site exploitation activities.
		3. Designate indigenous and/or host-nation forces, as appropriate,	Qualitative/ Subjective	As appropriate.

		as the lead at every possible opportunity for identity activities.		
		4. PN organizations not allowed to assist with gathering of forensic or other exploitation information and/or data, or evidence may be used, upon approval by the PN investigator, to primarily cordon and secure the site.	Qualitative/ Objective	Prior to identity and/or forensic data and/or other site exploitation activities.
		5. Identify local leaders and use them to assist in identifying the populace.	Quantitative /Objective	Once and as required.
		6. Create biometric enrollment events for future data mining.	Quantitative /Objective	Throughout operations.
	2. Personnel in the operational area are identified.	1. Ensure unit and/or patrol with handheld collection devices has taken enough extra charged batteries for completion of the mission.	Qualitative/ Subjective	Each collection event.
		2. Collect, to standard, identity information (e.g., personal documents, voter registration, driver's licenses, government databases) from individuals, to include detainees, within the operational area.	Quantitative /Objective	Once.
		3. At a minimum, fully biometrically enroll all military age males with full sets of fingerprints, full face photos, iris images, names, and all variants of names.	Quantitative /Objective	Once.
		4. Store identity information for all individuals in a designated authoritative database.	Quantitative /Objective	Every encounter.
		5. Ensure current watchlists and local alerts are loaded before mission execution.	Qualitative/ Objective	Prior to each mission.
		6. Send identity information to the Department of Defense authoritative database for match/no match.	Quantitative /Objective	Every encounter.
		7. Collect, preserve, store, analyze, and share forensic and other exploitation information and data.	Quantitative /Objective	Each incident.
	3. Intelligence functions produce identity intelligence products.	1. All-source intelligence analysts fuse and analyze all identity information from all sources (to include biometrics, personal identity documents, government database, forensics, and other exploitation). Record the following biographic data elements: address, occupation, tribal name, location of enrollment	Qualitative/ Subjective	Concurrent with all intelligence analysis.

		(military grid), to provide identities and trustworthiness attributes for each encountered individual.		
		2. Designate biometric named areas of interest through which persons of interest can be tracked.	Quantitative /Objective	As required during intelligence analysis.
		3. Use all sources of identity activities to support Intelligence operations (targeting individuals, cue other intelligence assets, ensure the correct target is engaged).	Qualitative/ Subjective	All opportunities to identify individuals.
	4. Personnel are vetted for trustworthiness; to determine whether they are a threat (military, nonmilitary, criminals, terrorists), friendly, or neutral.	1. Compare identity information against the biometric-enabled watchlist for match/no match and actions to take upon a match.	Quantitative /Objective	Every encounter.
		2. Use a badge system to identify local leaders and key personnel.	Quantitative /Objective	Once and as required.

Figure B-1. Example: Objective, Effects, and Indicators for Identity Information and Data (to Include Biometrics, Forensics, and Other Exploitation)

Example: Objective, Effects, and Indicators for Alien Migrant Interdiction Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Determine, and vet, identities of interdicted personnel for humanitarian missions and enforcement of US immigration laws at sea.	Assist, as necessary with other government departments or agencies (e.g., Federal Bureau of Investigation, Department of Homeland Security), and local authorities for identification and vetting of migrants as they attempt to enter the US from the sea.	1. Collect identity information and data from all individuals interdicted at sea. See Figure B-1.	See Figure B-1	See Figure B-1

Figure B-2. Example: Objective, Effects, and Indicators for Alien Migrant Interdiction Operations

Example: Objective, Effects, and Indicators for Base Access, Entry Control Points/Ports of Entry/Maritime Interception/Checkpoints				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Determine, and vet, identities of all personnel requesting access to bases, facilities, through checkpoints, points of entry, etc.	1. Authorized personnel are allowed access and exit.	1. Plan and establish checkpoints for identity verification. (yes/no)	Qualitative/ Subjective	As needed
		2. Canalize all traffic to checkpoints. (yes/no)	Qualitative/ Subjective	For all checkpoints
		3. Use "overwatch" to spot individuals trying to avoid checkpoints. (yes/no)	Qualitative/ Subjective	For all checkpoints
		4. Ensure up-to-date biometric-enabled watchlist, for the unit's operational area, is uploaded to the biometric handheld collection devices for verification.	Qualitative/ Objective	Every day
		5. Access authority receives personal identity documents from all individuals requesting access.	See Figure B-1	Once, during access authorization
		6. Fully enroll all personnel who will be allowed access to the installation.	Quantitative/ Objective See Figure B-1	Once, during access authorization
		7. Submit all enrollments to the Department of Defense authoritative database to complete the identification process for all locally employed personnel and require a match response.	Quantitative/ Objective See Figure B-1	Once during access authorization
		8. Issue authorized personnel a biometrically enabled access card.	Quantitative/ Objective	Once, upon authorization
	2. Unauthorized personnel are prevented from access or exit.	1. Biometrically screen all personnel entering or leaving the base to verify their identity, even if they possess an access card.	Quantitative/ Objective	Every incidence of entry or exit
		2. Plan for full Electronic Biometric Transmission Specification enrollments of suspect individuals.	Qualitative/ Objective	Every suspect individual attempting entry or exit

Figure B-3. Example: Objective, Effects, and Indicators for Base Access, Entry Control Points/Ports of Entry/Maritime Interception/Checkpoints

Example: Objective, Effects, and Indicators for Census Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Understand the identities of the population who live in, work in, or are passing through the operational area.	Provide the identities of the population to determine who normally lives in the operational area, who travels to the operational area for employment, are passing through the operational area, or are other individuals (e.g., threat forces, terrorists and/or criminals) who may be coercing the support of the local populations.	1. Conduct identity activities per Figure B-1.	See Figure B-1	Each census operation
		2. Have staging areas and standard operating procedures for collection operations.	Qualitative/ Subjective	Each census operation
		3. Maintain security at all times and ensure there are personnel search teams at the entry control point for the operation. If necessary, ensure your personnel search teams include females in order to search females.	Qualitative/ Subjective	Each census operation
		4. Listen to and understand residents' problems.	Qualitative/ Subjective	Each census operation
		5. Identify local leaders and use them to assist in the identification of the populace.	Qualitative/ Subjective	Each census operation
		6. Locate and identify every resident. (yes/no)	Qualitative/ Objective	Each census operation
		7. Visit and record every house and business.	Qualitative/ Objective	Each census operation
		8. Collect normal census and identification data from all individuals within the local operational area. (yes/no)	Qualitative/ Objective	During each census operation
		9. Use badges to identify local leaders, and key personnel.	Qualitative/ Objective	Each census operation
		10. Track persons of interest; unusual travel patterns may indicate unusual activities.	Qualitative/ Objective	During intelligence analysis and production of identity intelligence products

Figure B-4. Example: Objective, Effects, and Indicators for Census Operations

Example: Objective, Effects, and Indicators for Civil-Military Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Establish or reestablish the legitimacy of local authorities in activities that build or restore the partner nation's (PN's) capability and capacity. Improve PN capability and capacity to provide public services to its population, thereby enhancing legitimacy of the PN, enhancing force protection, and achieving the military objectives.	Accurately identify individuals and families receiving aid (medical care, food, water, material, jobs) through the use of identity activities, controls distribution and helps to eliminate waste and black marketeering, support of stability, counterinsurgency, and other activities dealing with "asymmetric" and "irregular" threats.	1. Conduct identity activities per Figure B-1.	See Figure B-1	Each civil-military operation (CMO).
		2. Provide joint force protection during identity activities as well as protection of the innocent population within the operational area.	Qualitative/ Subjective	Each CMO.
		3. Provide identity activities within access control missions (as described in the access control figure above).	Qualitative/ Objective	Each CMO.

Figure B-5. Example: Objective, Effects, and Indicators for Civil-Military Operations

Example: Objective, Effects, and Indicators for Countering Weapons of Mass Destruction				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Prevent the proliferation of weapons of mass destruction (WMD) by identifying personnel associated with various storage sites and involved in their trafficking.	1. Identify personnel associated with WMD sites.	1. Conduct identity activities per Figure B-1 for all individuals apprehended at WMD sites.	See Figure B-1	During every WMD operation
	2. Identify materials and personnel involved in WMD trafficking.	2. Conduct site exploitation at the site (as described in Figure B-30).	Qualitative/ Objective	During every WMD operation

Figure B-6. Example: Objective, Effects, and Indicators for Countering Weapons of Mass Destruction

Example: Objective, Effects, and Indicators for Chemical, Biological, Radiological, and Nuclear Response Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
To control access to chemical, biological, radiological, and nuclear (CBRN)-affected areas and to physically control access to residents and authorized personnel only.	Identity activities provide the necessary information for positive control of people to the affected areas.	1. Conduct identity activities per Figure B-1 for all individuals requesting access to CBRN sites.	See Figure B-1	Once for every CBRN incident
		2. Control access to the affected areas with a cordon. Match iris images for all personnel entering and exiting the area against the local database. (yes/no)	Qualitative/ Objective	Every entry/exit
		3. Conduct forensics and site exploitation activities (as described in Figure B-30).	Qualitative/ Objective	Every CBRN incident

Figure B-7. Example: Objective, Effects, and Indicators for Chemical, Biological, Radiological, and Nuclear Response Operations

Example: Objective, Effects, and Indicators for Cordon Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Discover selected personnel or materials.	1. Personnel are discovered and identified.	1. Conduct identity activities per Figure B-1 for all individuals within the cordoned site.	See Figure B-1	Each cordon mission.
		2. Use checkpoints in the cordon to canalize traffic and for collection of identity information via personal identity documents and biometric collection devices.	Qualitative/ Objective	All cordon operations
		3. Plan for positive or negative identification of personnel.	Qualitative/ Objective	All cordon operations
		4. Incorporate identity data into debriefs.	Qualitative/ Subjective	Post-mission cordon operations
		5. Biometrically enroll everyone, to include all wounded in action and killed in action.	Quantitative/ Objective	All cordon operations
	2. Materials are discovered and identified.	Plan for forensic material collection, to include latent fingerprints from materials, document and media exploitation (e.g., exploitation of pocket litter, found documents, found computer and cell phones, sim cards).	Qualitative/ Subjective	All cordon operations

Figure B-8. Example: Objective, Effects, and Indicators for Cordon Operations

Example: Objective, Effects, and Indicators for Counterdrug Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to contribute to the dissection of drugs, money, and terrorism.	1. Identify individuals and networks involved in drug activities.	Conduct identity activities per Figure B-1 for all individuals within the cordoned site.	See Figure B-1	During all counterdrug operations
	2. Joint force commanders (JFCs) are able to understand the flow of money, laundering of drug money, etc., supporting drug operations and terrorism.	Use identity activities to monitor, detect and interdict drug trafficking throughout the area of operations (especially border and transit zones).	Qualitative/ Subjective	During all counterdrug operations
	3. JFCs engage other countries to cooperate against the counterdrug trafficking and its second- and third-order effects.	Use identity activities to further provide an avenue of engagement for the source countries, providing a context for bilateral cooperation against trafficking and its second-and third-order effects.	Qualitative/ Subjective	During all counterdrug operations
	4. JFCs understand identities of individuals and networks conducting drug activities within banking and information technology (to include social media).	Use identity data from cyberspace sources and all other identity information in order to provide intelligence analysts cumulative data to dissect the links among drugs, money and terrorism, as well as the ancillary cottage industries of false documentation and human trafficking.	Qualitative/ Subjective	During all counterdrug operations

Figure B-9. Example: Objective, Effects, and Indicators for Counterdrug Operations

Example: Objective, Effects, and Indicators for Counter-Improvised Explosive Device Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Find and track threat, insurgents, and criminals.	1. Through identity activity support to intelligence analysis, individuals can be tied to various organizations and other human networks.	Conduct identity activities per Figure B-1 to identify individuals and networks involved in the preparation and use of improvised explosive devices (IEDs).	See Figure B-1	Every opportunity and upon discovery of IED kitchens, discovery of emplaced IEDs, and post-IED detonation
	2. Mobility (route clearing). Route clearing patrols identify explosives and other dangers near the route. Forensics is used to examine the device and the area. Identity activities are used to support site exploitation as well as biometric enrollment of nearby onlookers to determine if they are a threat.	Conduct identity activities per Figure B-1.	See Figure B-1	Discovery of emplaced IEDs, and post-IED detonation

Figure B-10. Example: Objective, Effects, and Indicators for Counter-Improvised Explosive Device Operations

Example: Objective, Effects, and Indicators for Combating Terrorism Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Identify bad actors to combat acts of terrorism.	Inclusion of identity activities in both antiterrorism and counterterrorism operations.	1. Conduct identity activities per Figure B-1 to identify individuals and networks involved in terrorism.	See Figure B-1	Throughout combating terrorism operations.
		2. Conduct site, and other forensic, exploitation to discover identity information about individuals and networks. See Figure B-1.	Qualitative/ Subjective	All opportunities

Figure B-11. Example: Objective, Effects, and Indicators for Combating Terrorism Operations

Example: Objective, Effects, and Indicators for Counterinsurgency Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Identify bad actors to combat insurgent activities.	Friendly, neutral, threat, and unknown-affiliated populations are identified.	Conduct identity activities per Figure B-1 to identify individuals and networks involved in insurgencies.	See Figure B-1	All COIN operations

Figure B-12. Example: Objective, Effects, and Indicators for Counterinsurgency Operations

Example: Objective, Effects, and Indicators for Countering Threat Networks				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Identify bad actors to dismantle threat networks.	Identify all individuals and associated threat networks impacting the operational environment.	1. Conduct identity activities per Figure B-1 to identify threat individuals and networks.	See Figure B-1	Throughout operations
		2. Conduct site, and other forensic, exploitation to discover identity information about individuals and networks.	See Figure B-1	All opportunities

Figure B-13. Example: Objective, Effects, and Indicators for Countering Threat Networks

Example: Objective, Effects, and Indicators for Cyberspace Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to anticipate, mitigate and deter cyberspace threats.	Identify individuals and threats operating in cyberspace.	1. Conduct identity activities per Figure B-1 to identify individuals and networks identified as threats within cyberspace (to include social media).	See Figure B-1	As available
		2. Use information technology/cyberspace operations standard operating procedures and tactics, techniques, and procedures to identify cyber-personas.	Qualitative/ Subjective	Throughout cyberspace operations
		3. Send cyber-persona information to intelligence for fusion with other identity information and data.	Quantitative/ Objective	Throughout cyberspace operations
	Cybersecurity measures are effective.	1. Biometrically enroll all network users.	Quantitative/ Objective	Each user
		2. Ensure all users sign and understand, appropriate information assurance forms.	Quantitative/ Objective	Each user

Figure B-14. Example: Objective, Effects, and Indicators for Cyberspace Operations

Example: Objective, Effects, and Indicators for Defense Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance defense objectives with identity activities.	Identity activities determine whether individuals within the operational environment are a threat (e.g., military, nonmilitary, criminal, terrorist, neutral).	Conduct identity activities per Figure B-1 to identify individuals and networks identified as threats.	See Figure B-1	During defense operations

Figure B-15. Example: Objective, Effects, and Indicators for Defense Operations

Example: Objective, Effects, and Indicators for Detainee Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Manage detainees.	1. Identify detained individuals.	1. Conduct identity activities per Figure B-1 to identify and vet detainees.	See Figure B-1	Throughout detainee operations
		2. Identify detainees.	Quantitative/ Objective	Upon detainment
		3. Use biometric enrollments to avoid identification mismatches due to changing and/or multiple versions of names.	Quantitative/ Objective	Upon detainment
	2. Support partner nation law enforcement by indicating linkages between an identified detainee and illicit activities.	1. Confirm whether each detainee is involved in illegal or criminal activities.	Quantitative/ Objective	Upon detainment
		2. Assist host nation prosecution of individuals through identity data matches and linkage to criminal activities.	Quantitative/ Objective	Upon detainment
	3. Manage detainees.	1. Track details of interactions with detainees throughout the detention process to include release (prevent the release of the wrong person).	Quantitative/ Objective	During detainment and prior to release
		2. Prepare for effective tactical questioning and/or interrogation by comparing the detainee's biometric information with the biometrics-enabled watchlist and other activities.	Quantitative/ Objective	During detainment

Figure B-16. Example: Objective, Effects, and Indicators for Detainee Operations

Example: Objective, Effects, and Indicators for Counter-Threat Finance Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Support partner nation (PN) investigations to identify, prosecute, and counter threat finance operations.	1. Discover identities of those individuals and networks involved in threat finance operations.	1. Conduct identity activities per Figure B-1 to identify and individuals suspected of unlawful threat finance activities.	See Figure B-1	Prior to information and/or data collection
		2. When identifying individuals, also consider virtual personas, and banking institutions databases to include linkage to networks, events, locations, and materials.	Quantitative/ Objective	Throughout operations
	2. Track financial transactions and financial activities.	1. Provide forensic exploitation of digital media; computer hard drives, cell phone histories and subscriber identity module cards (part of the document and media exploitation mission set).	Quantitative/ Objective	Upon discovery of threat finance activities and/or persons/networks
		2. Identify, and plan for, opportunities to interdict funding of illicit activities.	Qualitative/ Subjective	In coordination with PNs and discovery of illicit activities
		3. Use forensic techniques to trace financial records and identify financiers.	Quantitative/ Objective	In coordination with PNs and discovery of illicit activities

Figure B-17. Example: Objective, Effects, and Indicators for Counter-Threat Finance Operations

Example: Objective, Effects, and Indicators for Foreign Internal Defense Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance foreign internal defense (FID) objectives through identity activities.	Identify and vet individuals to support the protection of the host nation (HN) against subversion, lawlessness, insurgency, terrorism, and other threats to their security.	1. Engage with host nation (HN) authorities and provide education on the usefulness of identity capabilities (such as biometrics, forensics, and document and media exploitation).	Qualitative/ Subjective	At initiation of FID operations, training, exercises, etc.
		2. Ensure bilateral agreements are in place between the US and the HN in order for US forces to collect, store, and share identity (to include biometric and forensic) information and data.	Qualitative/ Objective	Prior to FID operations; if not in place, quickly develop and approve agreements with specifics
		3. Store identity data into a local database.	Quantitative/ Objective	Upon establishment of agreements; prior to initiation of

				training, exercises, etc.
		4. Verify the identities of individuals receiving US led training (especially through the use of biometrics), and vet, the individual trained against the biometric-enabled watchlist, the Department of Defense authoritative biometrics repository, and/or the local database.	Quantitative/ Objective	Upon establishment of agreements; prior to initiation of training, exercises, etc.

Figure B-18. Example: Objective, Effects, and Indicators for Foreign Internal Defense Operations

Example: Objective, Effects, and Indicators for Human Trafficking				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to oppose prostitution, forced labor, and any related activities contributing to the phenomenon of trafficking in persons (TIP).	Reduce the level of human trafficking in commanders' operational areas.	1. Ensure the identification of personnel involved in TIP (victim/suspect).	Quantitative/ Qualitative	Each encounter
		2. Biometrically enroll all TIP violators.	Quantitative	Each encounter
		3. Plan for identity data collection in the operation order/fragmentary orders for any TIP activities.	Qualitative/ Subjective	As available

Figure B-19. Example: Objective, Effects, and Indicators for Human Trafficking

Example: Objective, Effects, and Indicators for Foreign Humanitarian Assistance				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance foreign humanitarian assistance (FHA) objectives with identity activities.	1. Joint forces are protected from criminal and possible threat activities.	1. Plan to identify potential persons of interest (Watchlisted individuals).	Qualitative/ Subjective	Prior to execution of FHA operations
		2. Detain anyone on the biometric-enabled watchlist (if used) or who has had a latent print recovered from a site of anti-multinational force activities.	Quantitative/ Objective	Every encounter
		3. Plan for full biometrics enrollments and verifications/screenings.	Qualitative/ Objective	Prior to execution of FHA operations
		4. Ensure authorities and agreements are in place with host nations for Department of Defense collection, storage, and sharing of identity information in the partner nations (PNs).	Qualitative/ Objective	Prior to execution of FHA operations
		5. Integrate the identification,	Quantitative/	Every encounter

		verification, and vetting of individuals to better provide joint force protection.	Objective	
		6. Use identity information with regards to base camp organization for access control.	Quantitative/ Objective	Every encounter
	2. Families are reunited due to FHA.	Reunite families after a disaster (using deoxyribonucleic acid).	Quantitative/ Objective	For every separated individual
	3. FHA resources are provided to all persons in need.	1. Biometrically enroll all recipients of FHA to ensure no "double dipping" into FHA resources.	Quantitative/ Objective	Every encounter
		2. Collect identity data from personal identity documents and PN databases (e.g., driver's licensing, voter registration).	Quantitative/ Objective	Every encounter
		3. Provide for more efficient records/organization of individual profiles through the use of identity information.	Qualitative/ Subjective	Every encounter
		4. Use identity data for placement and tracking of individuals and resources provided to each individual.	Quantitative/ Objective	Every encounter
		5. Share identity information and data with other agencies and multination partners for the efficient pursuit of the FHA purposes.	Quantitative/ Objective	Every encounter

Figure B-20. Example: Objective, Effects, and Indicators for Foreign Humanitarian Assistance

Example: Objective, Effects, and Indicators for Intelligence				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Support identity intelligence products.	Identity activity information and data are integrated throughout all-source intelligence analysis and products.	1. Conduct identity activities to support intelligence analysis per Figure B-1.	See Figure B-1	Throughout military operations
		2. Use all sources of identity activities to support Intelligence operations (targeting individuals, cue other intelligence assets, ensure the correct target is engaged).	Qualitative/ Subjective	All opportunities to identify individuals

Figure B-21. Example: Objective, Effects, and Indicators for Intelligence

Example: Objective, Effects, and Indicators for Logistics				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Identity activities enhance logistics support to joint force commanders (JFCs) throughout the competition continuum.	Identity activities are used to support force freedom of movement, disposition of material, contractor vetting, and tracking of services given to personnel.	1. Conduct identity activities to support logistics per Figure B-1.	See Figure B-1	Throughout JFC operations
		2. Biometrically enroll, and vet, all Department of Defense contractors and locally employed personnel.	Quantitative/ Objective	Each contractor and locally employed personnel
		3. Require biometrics validation to receive payment.	Objective	Per standard operating procedures

Figure B-22. Example: Objective, Effects, and Indicators for Logistics

Example: Objective, Effects, and Indicators for Military Police Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to enhance military police (MP) operations, provide support to identity intelligence and criminal intelligence, law enforcement missions as well as possible future prosecutions.	Individuals and/or networks are identified, verified, and vetted to determine whether they are threats of any type.	1. Conduct identity activities to support noncombatant evacuation operations per Figure B-1.	See Figure B-1	During all military operations
		2. Provide MP and exploitation analyses for possible linkage of identified individual and/or network threats to unlawful events, materials, and locations.	Qualitative/ Objective. Also see Figures B-1 and B-30 (Site Exploitation)	During all military operations

Figure B-23. Example: Objective, Effects, and Indicators for Military Police Operations

Example: Objective, Effects, and Indicators for Noncombatant Evacuation Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance noncombatant evacuation operations (NEOs).	Use identity activities to identify those eligible for NEO.	Conduct identity activities to support NEOs per Figure B-1.	See Figure B-1	Each encounter

Figure B-24. Example: Objective, Effects, and Indicators for Noncombatant Evacuation Operations

Example: Objective, Effects, and Indicators for Offense Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance offense operations objectives with identity activities.	Identity activities determine whether individuals within the operational environment are a threat (military, non-military, criminal, terrorist, neutral).	1. Conduct identity activities per Figure B-1.	See Figure B-1	Throughout offense operations as appropriate.
		2. Ensure detainees within the area of responsibility and/or suspect individuals are identified and vetted for trustworthiness.	See Figure B-1	Throughout offense operations as appropriate.

Figure B-25. Example: Objective, Effects, and Indicators for Offense Operations

Example: Objective, Effects, and Indicators for Peace Operations				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance peace operations objectives with identity activities.	Identities of individuals and/or networks are verified and vetted for trustworthiness.	1. Conduct identity activities, per Figure B-1, for partner nation (PN) individuals, networks, local police, military, and security forces, as well as those to receive training.	See Figure B-1	Throughout peace operations as appropriate
		2. Use identity activities as a means to work more closely with PN forces and organizations managing food, water, medical care, funds, contractor, etc.	Qualitative/ Subjective	As mission allows
		3. Inform commanders about the true background of some of PN personnel, potential hires, civilian population (e.g., medical).	Qualitative/ Subjective	Each applicant

Figure B-26. Example: Objective, Effects, and Indicators for Peace Operations

Example: Objective, Effects, and Indicators for Personnel Recovery				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to enhance personnel recovery operations.	Identify recovered persons (alive, deceased, or unconscious).	1. Conduct identity activities, per Figure B-1, for recovered individuals (alive, deceased, or unconscious).	See Figure B-1	Throughout operations
		2. Positively identify a person that is alive, deceased (regardless of the integrity of the body), or if the individual is unconscious.	Quantitative/ Objective	Each encounter

Figure B-27. Example: Objective, Effects, and Indicators for Personnel Recovery

Example: Objective, Effects, and Indicators for Personnel Screening and Vetting				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance force protection and local security.	Identify, verify identities, and vet personnel (threat, friendly, or neutral) to determine allegiance, background or suitability for credentialing, decide access to a protected area (e.g., base, town, or to possibly segregate populations to enhance security.	Conduct identity activities, per Figure B-1, for personnel.	See Figure B-1	Throughout operations

Figure B-28. Example: Objective, Effects, and Indicators for Personnel Screening and Vetting

Example: Objective, Effects, and Indicators for Populace and Resources Control Measures				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance the management of local populations during operations throughout the competition continuum.	Identity, verify, and vet the identities of the population in order to deny freedom of movement and provide resources to designated population.	1. Conduct identity activities, per Figure B-1, for personnel.	See Figure B-1	Throughout operations
		2. Plan, and establish, checkpoints for identity verification.	Quantitative/ Objective	Throughout operations

Figure B-29. Example: Objective, Effects, and Indicators for Populace and Resources Control Measures

Example: Objective, Effects, and Indicators for Site Exploitation				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Use identity activities to enhance site exploitation (SE) for identity intelligence and law enforcement missions as well as possible future prosecutions.	Properly record and preserve the evidence.	1. Conduct identity activities per Figure B-1.	See Figure B-1	See Figure B-1
		2. Collect and preserve latent fingerprints. (yes/no)	Qualitative/ Objective	Each occurrence
		3. Compare latent fingerprints against authoritative repositories and the biometric-enabled watchlist. (yes/no)	Qualitative/ Objective	Each occurrence
		4. Add identity information from this specific SE to dossiers on involved individuals. (yes/no)	Qualitative/ Objective	Each occurrence

		5. Security teams ask individuals at the SE site to show their identification documents as well as enrolled/matched with biometric devices.	Qualitative/ Objective	Each occurrence
		6. Tag, record, package, and transport useful artifacts, electronic data/media, fibers, and other documents to the nearest forensic laboratory. (yes/no)	Qualitative/ Objective	Each occurrence
		7. Follow strict chain-of-custody policies for all artifacts and documents. (yes/no)	Qualitative/ Objective	Each occurrence
		8. Retain and exploit all useful artifacts and documents for intelligence value and/or prosecution efforts. (yes/no)	Qualitative/ Objective	Each occurrence

Figure B-30. Example: Objective, Effects, and Indicators for Site Exploitation

Example: Objective, Effects, and Indicators for Stability Activities				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance stabilization, security, transition and reconstruction operations.	Identify, verify, and vet individual identities in order to evaluate trustworthiness and identify threats (criminals, terrorists, insurgents), friendly, and neutral entities and/or networks within the population.	1. Conduct identity activities per Figure B-1.	See Figure B-1	See Figure B-1
		2. Use identity activities as a means to work more closely with host nation forces (e.g., elections, food, water, medical care, funds, contractor employment, and distribute resources).	Quantitative/ Subjective	As mission allows
		3. Inform commanders about the true background of some of their personnel, potential hires, civilian population (e.g., medical).	Qualitative/ Subjective	Each applicant

Figure B-31. Example: Objective, Effects, and Indicators for Stability Activities

Example: Objective, Effects, and Indicators for Support to Targeting				
Objective	**Effect**	**Indicator**	**Data Category**	**Frequency (example)**
Enhance targeting.	1. Identity activities determine high-value individuals that may be nominated for targeting.	1. Conduct identity activities per Figure B-1.	See Figure B-1	See Figure B-1
		2. After consideration of all operational factors, and staff input, joint force commanders identify potential high-value individuals for targeting (lethal and/or non-lethal effects).	Qualitative/objective	All operations throughout the competition continuum.
	2. During or post-targeting mission, identity activities are used in the verification of the identity of each targeted individual.	3. Use biometrics to verify target(s).	Quantitative/ Objective	As occurs

Figure B-32. Example: Objective, Effects, and Indicators for Support to Targeting

Intentionally Blank

APPENDIX C
REFERENCES

The development of *Joint Doctrine Note 3-19* is based upon the following references:

1. General

a. Title 5, USC.

b. Title 10, USC.

c. Title 50, USC.

d. *National Security Strategy of the United States of America.*

e. (U) *2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge.*

f. *National Intelligence Strategy of the United States of America.*

g. (U) *National Military Strategy of the United States of America, 2018.*

h. *National Strategy for Counterterrorism of the United States of America.*

i. *National Strategy to Combat Transnational Organized Crime.*

j. *National Strategy for Homeland Security.*

k. HSPD-6, *Integration and Use of Screening Information to Protect Against Terrorism.*

l. HSPD-10, *Biodefense for the 21st Century.*

m. HSPD-11, *Comprehensive Terrorist-Related Screening Procedures.*

n. NSPD-59/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security.*

o. PPD 18, *Maritime Security Policy.*

p. PPD 23, *Security Sector Assistance.*

q. EO 12333, *United States Intelligence Activities.*

r. ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*

s. ICD 302, *Document and Media Exploitation.*

2. Department of Defense Publications

a. DODD 300.05, *Stabilization.*

b. DODD 3000.07, *Irregular Warfare (IW).*

c. DODD 3300.03, *DOD Document and Media Exploitation (DOMEX).*

d. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.*

e. DODD 5205.14, *DOD Counter Threat Finance (CTF) Policy.*

f. DODD 5205.15E, *DOD Forensic Enterprise (DFE).*

g. DODD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations.*

h. DODD 5240.01, *DOD Intelligence Activities.*

i. DODD 8521.01E, *DOD Biometrics.*

j. DODI O-3300.04, *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI).*

k. DODI 5505.14, *Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders.*

l. DODI 5525.18, *Law Enforcement Criminal Intelligence (CRIMINT) in DOD.*

m. DODM 5200.1, *DOD Information Security Program, Volumes 1-4.*

n. DOD 5400.11-R, *Department of Defense Privacy Program.*

3. Chairman of the Joint Chiefs of Staff Publications

a. JP 1, Volume 1, *Joint Warfighting.*

b. JP 2-0, *Joint Intelligence.*

c. JP 3-0, *Joint Operations.*

d. JP 3-05, *Special Operations.*

e. JP 3-06, *Joint Urban Operations.*

f. JP 3-07, *Stability.*

g. JP 3-07.3, *Peace Operations.*

h. JP 3-07.4, *Counterdrug Operations.*

i. JP 3-08, *Interorganizational Cooperation.*

j. JP 3-10, *Joint Security Operations in Theater*.

k. JP 3-12, *Cyberspace Operations.*

l. JP 3-16, *Multinational Operations*.

m. JP 3-20, *Security Cooperation.*

n. JP 3-22, *Foreign Internal Defense*.

o. JP 3-24, *Counterinsurgency*.

p. JP 3-25, *Countering Threat Networks.*

q. JP 3-26, *Combating Terrorism.*

r. JP 3-29, *Foreign Humanitarian Assistance*.

s. JP 3-40, *Countering Weapons of Mass Destruction.*

t. JP 3-50, *Personnel Recovery*.

u. JP 3-57, *Civil-Military Operations.*

v. JP 3-63, *Detainee Operations.*

w. JP 3-68, *Noncombatant Evacuation Operations.*

x. JP 4-10, *Operational Contract Support.*

y. JP 5-0, *Joint Planning.*

4. Service, Multi-Service, and Combatant Command Publications

a. Army Doctrine Publication 2-0, *Intelligence*.

b. Army Doctrine Publication 3-0, *Operations.*

c. Army Doctrine Publication 3-07, *Stability*.

d. Army Doctrine Publication 3-37, *Protection*.

e. Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques.*

f. ATP 2-22.82, *Biometrics Enabled Intelligence (U).*

g. COMDTINST M16247.1, *US Coast Guard Maritime Law Enforcement Manual.*

h. Field Manual (FM) 2-0, *Intelligence.*

i. FM 3-24/Marine Corps Warfighting Publication 3-02, *Insurgencies, and Countering Insurgencies.*

j. FM 3-55, *Information Collection.*

k. Marine Corps Doctrinal Publication (MCDP) 1-0, *Marine Corps Operations.*

l. MCDP 5, *Planning.*

m. Marine Corps Order 5530.17, *Marine Corps Identity Operations (IdOps).*

n. NTTP 3-07.4/COMDINST M16247.4, *Maritime Counterdrug and Alien Migration Interdiction Operations.*

o. NTTP 3-07.11M/CGTTP 3-93.3, *Visit, Board, Search, and Seizure Operations.*

p. USSOCOM Publication 1, *Doctrine for Special Operations.*

q. USSOCOM Directive 525-16 (S/NF), *Preparation of the Environment.*

r. USSOCOM Directive 525-40, *Identity Intelligence Operations.*

s. USSOCOM Directive 525-89 (S/NF), *Unconventional Warfare.*

5. Allied Publications

a. Allied Joint Publication 2.5, *Captured Persons, Materiel and Documents.*

b. Allied Joint Publication 3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices.*

c. Allied Intelligence Publication 15, *Countering Threat Anonymity: Biometrics in Support of Operations & Intelligence.*

d. NATO Standardization Agreement 4715, *NATO Biometrics Data, Interchange, Watchlisting and Reporting.*

6. Other Sources

a. Flynn, MG Michael, M. Pottinger, and P. Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Center for New American Security (January 2010).

b. McFate, Montgomery, and Steve Fondacaro. “Reflections on the Human Terrain System During the First Four Years,” *PRISM Journal,* Vol. 2, No. 4 (September 2011).

c. Olson, Wm. J. “War Without a Center of Gravity: Reflections on Terrorism and Post- Modern War,” *Small Wars and Insurgencies*, Vol. 18, No. 4 (December 2007).

d. *US Military Response to the 2010 Haiti Earthquake*. RAND Arroyo Center, 2013.

e. Networks and Netwars The Future of Terror[ism], Crime, and Militancy, Edited by John Arquilla, David Ronfeldt.

f. Alda, E., and J. L. Sala. Links Between Terrorism, Organized Crime and Crime: The Case of the Sahel Region. *Stability: International Journal of Security and Development*, Vol. 3, No. 1, Article 27, pp.1-9.

g. Everton, Sean F. *Disrupting Dark Networks.* Cambridge University Press, 2012.

Intentionally Blank

GLOSSARY

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

ABIS	Department of Defense Automated Biometric Identification System
AOR	area of responsibility
ATP	Army techniques publication
BAT-A	Biometrics Automated Toolset-Army
BEI	biometrics-enabled intelligence
BEWL	biometric-enabled watchlist
BI2R	Biometric Identity Intelligence Resource (USA)
BICES	battlefield information collection and exploitation system (NATO)
C2	command and control
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCIR	commander's critical information requirement
CCMD	combatant command
CCP	combatant command campaign plan
CDRUSSOCOM	Commander, United States Special Operations Command
CEXC	combined explosives exploitation cell
CF	conventional forces
CGTTP	Coast Guard tactics, techniques, and procedures
C-IED	counter-improvised explosive device
CMO	civil-military operations
COA	course of action
COM	chief of mission
COMDTINST	Commandant of the Coast Guard instruction
CONOPS	concept of operations
CONUS	continental United States
CRIMINT	criminal intelligence
DFSC	Defense Forensic Science Center
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNA	deoxyribonucleic acid
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODM	Department of Defense manual
DOMEX	document and media exploitation
DONISIS	Department of the Navy Identification and Screening Information System
DOS	Department of State

EA	executive agent
EAC	exploitation analysis cell
ECP	entry control point
EFEC	expeditionary forensics exploitation capability
EO	executive order
EOD	explosive ordnance disposal
EU	European Union
EXU	expeditionary exploitation unit
FBI	Federal Bureau of Investigation (DOJ)
FEI	forensic-enabled intelligence
FHA	foreign humanitarian assistance
FID	foreign internal defense
FM	field manual (USA)
FXL	forensics exploitation laboratory (USA)
FXT	forensic exploitation team
HN	host nation
HSPD	homeland security Presidential directive
HVI	high-value individual
I2	identity intelligence
I2PO	Identity Intelligence Project Office (DIA)
I2WD	Intelligence and Information Warfare Directorate (USA)
IC	intelligence community
ICD	intelligence community directive
IDENT	Automated Biometric Identification System (DHS)
IDS	Identity Dominance System (USN)
IDS-MC	Identity Dominance System-Marine Corps (USMC)
IED	improvised explosive device
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
JDEC	joint document exploitation center
JDIS	Joint Deoxyribonucleic Acid Index System
JFC	joint force commander
JIOC	joint intelligence operations center
JIPOE	joint intelligence preparation of the operational environment
JOA	joint operations area
JP	joint publication
JPP	joint planning process
JS	Joint Staff
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communication System

MAGTF	Marine air-ground task force
MCDP	Marine Corps doctrinal publication
MEF	Marine expeditionary force
MNF	multinational force
MOC	memorandum of cooperation
MOE	measure of effectiveness
MOP	measure of performance
NATO	North Atlantic Treaty Organization
NCB	national central bureau
NCIS	Naval Criminal Investigative Service
NDIS	National Deoxyribonucleic Acid Index System (FBI)
NDP	national disclosure policy
NGI	Next Generation Identification (FBI)
NGO	nongovernmental organization
NMEC	National Media Exploitation Center
NSC	National Security Council
NSPD	national security Presidential directive
NTTP	Navy tactics, techniques, and procedures
OE	operational environment
OCS	operational contract support
OPCON	operational control
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense
PCA	Posse Comitatus Act
PIR	priority intelligence requirement
PN	partner nation
POW	prisoner of war
PPD	Presidential policy directive
ROE	rules of engagement
RUF	rules for the use of force
SDO/DATT	senior defense official/defense attaché
SECARMY	Secretary of the Army
SecDef	Secretary of Defense
SFA	security force assistance
SIPRNET	SECRET Internet Protocol Router Network
SJA	staff judge advocate
SOF	special operations forces
SOFEX	special operations forces exploitation
SSA	security sector assistance

TEDAC	Terrorist Explosive Device Analytical Center (FBI)
TF	task force
TSOC	theater special operations command
TTP	tactics, techniques, and procedures
UN	United Nations
USC	United States Code
USCG	United States Coast Guard
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USG	United States Government
USSOCOM	United States Special Operations Command
VBSS	visit, board, search, and seizure
WMD	weapons of mass destruction

JOINT
CHIEFS OF STAFF