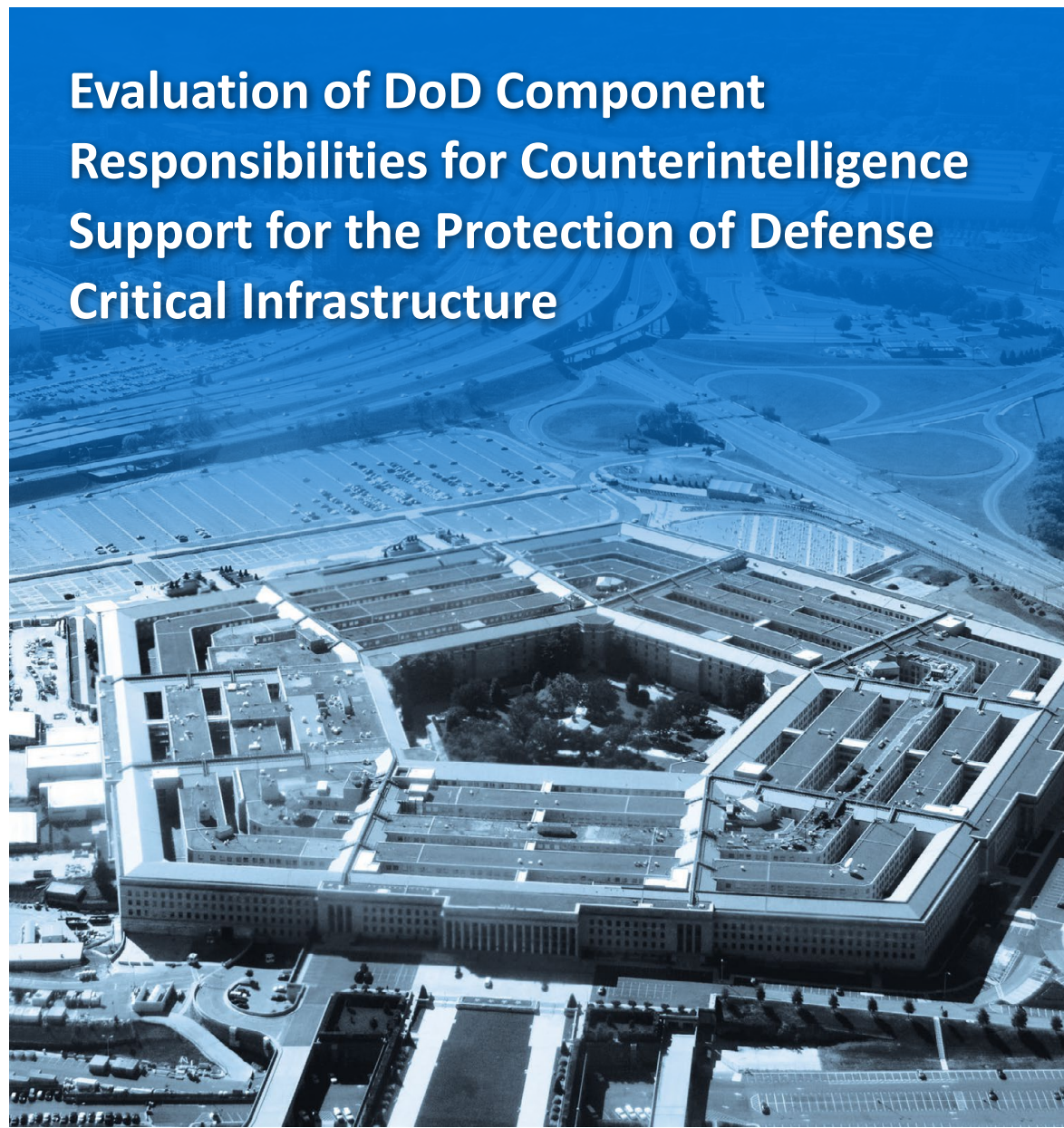




INSPECTOR GENERAL

U.S. Department of Defense

APRIL 5, 2019



Evaluation of DoD Component Responsibilities for Counterintelligence Support for the Protection of Defense Critical Infrastructure

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE





Results in Brief

Evaluation of DoD Component Responsibilities for Counterintelligence Support for the Protection of Defense Critical Infrastructure

April 5, 2019

Objective

We determined whether DoD Components assigned responsibilities for counterintelligence (CI) support and managed the Integrated Management Group to protect defense critical infrastructure.

Background

The Department of Homeland Security defines critical infrastructure as “essential services that underpin American society,” such as energy systems, banking and finance systems, chemical facilities, the DoD Information Network, and nuclear power systems. Critical infrastructure is defined as assets so vital that their exploitation, incapacitation, or destruction would have a debilitating effect on national security, the U.S. economy, public health or safety, or any combination thereof. According to Homeland Security Presidential Directive (HSPD)-7, although it is not possible to eliminate all vulnerabilities to critical infrastructure and key resources throughout the country, improvements in security can mitigate, neutralize, or prevent the impact of adversarial attacks on critical infrastructure. HSPD-7 required Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Presidential Policy Directive (PPD)-21, superseded HSPD-7, and requires the DoD to continue efforts to meet requirements established by HSPD-7.

Background (cont’d)

The DoD issued DoD Directive 3020.40, “Defense Critical Infrastructure Program,” August 19, 2005, implementing DoD support to critical infrastructure through the Defense Critical Infrastructure Program (DCIP), a DoD risk management program that sought to ensure the availability of networked assets—interconnected assets that rely on each other to provide a service—critical to DoD missions.

DoD Directive 3020.40 first introduced the concept of defense infrastructure sector lead agents (DISLAs), who were responsible for the identification, prioritization, and protection of essential DoD services and infrastructure within 10 defined infrastructure sectors, such as space, transportation, and intelligence.

In 2016, the DoD updated DoD Directive 3020.40 and changed DCIP to a line of effort under the Mission Assurance Program. According to DoD Directive 3020.40, the mission assurance program is designed to sustain programming, resources, functions, and activities supporting responsibilities formerly under DCIP. DoD Directive 3020.40 states that mission assurance is the DoD-wide process to identify, assess, manage, and monitor the risks to strategic missions. However, the 2016 DoD Directive 3020.40 does not reference requirements for DoD sectors or DISLAs.

In addition, DoD Instruction 5240.19, “Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP),” January 21, 2014, requires DoD CI components to assign CI support to the DoD sectors and their corresponding DISLAs within the purview of previously established Defense sectors of responsibility. DoD Instruction 5240.19 requires that CI activities be conducted in accordance with DoD Directive 3020.40 and DoD Directive 5243.01, “Under Secretary of Defense for Intelligence (USD[I]),” October 24, 2014, and that CI organizations provide comprehensive and timely reporting of foreign intelligence entity threats, incidents, events, and trends to essential DoD services and infrastructure and the DoD Components.



Results in Brief

Evaluation of DoD Component Responsibilities for Counterintelligence Support for the Protection of Defense Critical Infrastructure

Finding

USD(I) did not assign responsibilities for CI coverage of critical assets and facilities previously managed by DISLAs. This occurred because, although DISLA positions were eliminated by DoD Directive 3020.40 in 2016, USD(I) has not yet updated DoD Instruction 5240.19 to assign CI responsibilities that were previously aligned to support DISLAs and their corresponding sectors. As a result, DoD CI support provided through efforts such as threat awareness briefings, CI inquiries, and support to the DoD foreign visitors program may not consistently identify CI threats to essential DoD services and infrastructure. Without current and clear guidance, it is difficult for DoD Components to provide consistent and comprehensive CI support to essential DoD services and infrastructure.

In addition, from 2015 to 2018, the Defense Intelligence Agency (DIA) did not manage the Integrated Management Group to support CI functional management and integration of CI support, as required by DoD Instruction 5240.19. According to DIA officials, this occurred because attempts to reinvigorate the Integrated Management Group were hampered by limited personnel. As a result, the DoD may not be adequately integrating and coordinating CI support for essential DoD services and infrastructure, which could result in duplicative CI efforts or insufficient CI coverage to these assets.

Recommendations

We recommend that the Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, revise all applicable DoD policies to ensure the protection of essential DoD services and infrastructure.

We recommend that the Director of the Office of Community Coordination, Defense Intelligence Agency, reestablish and appoint a chair and deputy chair to the Defense Critical Infrastructure Line of Effort Integrated Management Group as required by DoD Instruction 5240.19, to enhance counterintelligence functional management and integration of counterintelligence support to the essential DoD services and infrastructure line of effort, as required by DoD Instruction 5240.19.

Management Comments and Our Response

The Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, agreed with the recommendation, stating that DoD counterintelligence policy will be rewritten by April 2020 to reflect the changes to DoD Directive 3020.40 and DoD Instruction 3020.45, to ensure that counterintelligence responsibilities are aligned to critical asset owners. We consider this recommendation resolved but open. We will close this recommendation once we receive and review the updated policy.

Management comments received by the Director of the Office of Community Coordination, Defense Intelligence Agency, agreed with the recommendation, stating that an Integrated Management Group chair was appointed in August 2018, and that a volunteer from the Integrated Management Group members will be requested to serve as the deputy chair during the March 28, 2019, Integrated Management Group meeting. Therefore, the recommendation is resolved but will remain open until we receive appointment letters for the Integrated Management Group chair and deputy chair, along with Integrated Management Group meeting minutes.

Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence	None	1	None
Director of the Office of Community Coordination, Defense Intelligence Agency	None	2	None

Note: The following categories are used to describe agency management’s comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.





**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500**

April 5, 2019

MEMORANDUM FOR DIRECTOR FOR DEFENSE INTELLIGENCE (INTELLIGENCE
AND SECURITY), OFFICE OF THE UNDER SECRETARY OF
DEFENSE FOR INTELLIGENCE
DIRECTOR, OFFICE OF COMMUNITY COORDINATION, DEFENSE
INTELLIGENCE AGENCY

SUBJECT: Evaluation of DoD Component Responsibilities for Counterintelligence
Support for the Protection of Defense Critical Infrastructure
(Report No. DODIG-2019-071)

We are providing this report for your information and use. We conducted this evaluation in accordance with the "Quality Standards for Inspection and Evaluation," published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency.

We considered management comments on the draft of this report when preparing the final report. Comments from the Chief of Staff and the Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, and the Director of the Office of Community Coordination, Defense Intelligence Agency, addressed all specifics of the recommendations and conformed to the requirements of DoD Instruction 7650.03; therefore, we do not require additional comments.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-9187, DSN 312-664-9187.

A handwritten signature in blue ink, appearing to read "MJR", is positioned above the name of the Deputy Inspector General.

Michael J. Roark
Deputy Inspector General for
Evaluations

Contents

Introduction

Objective	1
Background	1

Finding. DoD Counterintelligence Policy Was Not Aligned With Current Mission Assurance Policy to Protect Essential DoD Services and Infrastructure

7

USD(I) Did Not Assign Responsibilities for Counterintelligence	
Coverage of Critical Assets and Facilities	7
The DIA Did Not Manage the Integrated Management Group, as Required by DoD Policy	10
Recommendations, Management Comments, and Our Response	11

Appendixes

Appendix A. Scope and Methodology	13
Computer-Processed Data	14
Prior Coverage	14
Appendix B. Mission Assurance Construct Process Chart	15

Management Comments

Chief of Staff, Office of the Under Secretary of Defense for Intelligence	16
Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence	17
Director of the Office of Community Coordination, Defense Intelligence Agency	19

Acronyms and Abbreviations

20

Introduction

Objective

We determined whether DoD Components assigned responsibilities for counterintelligence (CI) support and managed the Integrated Management Group to protect defense critical infrastructure, hereafter referred to as essential DoD services and infrastructure.

Background

The Department of Homeland Security classifies critical infrastructure as “essential services that underpin American society,” such as energy systems, banking and financial systems, chemical facilities, and nuclear power systems. Critical infrastructure is defined as assets that are so vital that their exploitation, incapacitation, or destruction would have a debilitating effect on national security, the U.S. economy, public health or safety, or any combination thereof. According to Homeland Security Presidential Directive (HSPD)-7, although it is not possible to eliminate all of the vulnerabilities related to critical infrastructure and key resources throughout the country, improvements in security can mitigate, neutralize, or prevent the impact of adversarial attacks on critical infrastructure.¹ HSPD-7 required Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them.

In addition, the issuance of Presidential Policy Directive (PPD)-21, which superseded HSPD-7, charges the Secretary of Homeland Security to “promote a national unity of effort” and coordinate the “security and resilience of the Nation’s critical infrastructure.”²

The DoD has two roles for providing critical infrastructure protection: first as a Federal department and second as a sector-specific agency for one of 16 national infrastructure sectors—the Defense Industrial Base (DIB).³

As a Federal department, the DoD has both departmental and national responsibilities. Departmental responsibilities include the identification, prioritization, assessment, remediation, and protection of essential DoD services and infrastructure.

¹ Homeland Security Presidential Directive 7, “Critical Infrastructure Identification, Prioritization, and Protection,” December 7, 2003.

² Presidential Policy Directive (PPD)-21, “Critical Infrastructure Security and Resilience,” February 12, 2013.

³ Sector-specific denotes the agency responsible for a sector. The DoD is the sector-specific Agency for the DIB sector. The DIB sector enables research, development, design, production, delivery, and maintenance of military weapons systems, sub-systems, and components or parts to meet U.S. military requirements.

As a sector-specific Agency for the DIB, the DoD supports the Department of Homeland Security in executing its national responsibilities. The DoD's national responsibilities specific to the DIB are detailed in the National Infrastructure Protection Plan, which states that the DIB sector provides defense-related products and services that are essential to the mobilization, deployment, and sustainment of military operations. Public and private sector partners in each of the 16 critical infrastructure sectors and the state, local, tribal, and territorial government community have developed a sector-specific plan for the National Infrastructure Protection Plan that focuses on the unique operating conditions and risk landscape within each sector.

The DoD's Implementation of Critical Infrastructure Protection Policy

DoD Directives 3020.40 and 3020.45 established requirements for the implementation of critical infrastructure protection under a DoD program. DoD Instruction 5240.19 implements CI support to the DoD's critical infrastructure program (DCIP).⁴

DoD Directive 3020.40 Has Changed Over Time

The DoD issued DoD Directive 3020.40 in 2005, implementing DoD support to critical infrastructure through the DCIP, a DoD risk management program that sought to ensure the availability of networked assets—interconnected assets that rely on each other to provide a service—critical to DoD missions. The 2005 DoD Directive 3020.40 first introduced the concept of defense infrastructure sector lead agents (DISLAs), who were responsible for the identification, prioritization, and protection of essential DoD services and infrastructure within 10 defined infrastructure sectors, such as space, transportation, and intelligence. In 2010, the DoD renamed, revised, and updated DoD Directive 3020.40 and further emphasized the role of the DISLAs.⁵

⁴ DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005; DoD Directive 3020.40, "DoD Policy And Responsibilities For Critical Infrastructure," January 14, 2010; DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, With Change 1, September 11, 2018; DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018; And DoD Instruction 5240.19, "Counterintelligence Support To The Defense Critical Infrastructure Program (DCIP)," January 21, 2014, With Change 1, August 17, 2017.

⁵ DoD Directive 3020.40, "DoD Policy and Responsibility for Critical Infrastructure," January 10, 2010.

Former Defense Infrastructure Sectors

According to the 2010 DoD Directive 3020.40, Defense infrastructure sectors were associations within the DCIP that encompassed defense networks, assets, and associated dependencies, such as interconnected networks or assets that rely on each other to provide a service, that performed similar functions within the DoD and that were essential to the execution of the National Defense Strategy. The 10 former DISLAs and their former sector responsibilities were:

- Defense Industrial Base—the Director of the Defense Contract Management Agency;
- Financial Services—the Director of the Defense Finance and Accounting Service;
- DoD Information Networks (formerly the Global Information Grid)—the Director of the Defense Information Systems Agency;
- Health Affairs—the Assistant Secretary of Defense (Health Affairs);
- Intelligence, Surveillance, and Reconnaissance—the Director of the Defense Intelligence Agency;
- Logistics—the Director of the Defense Logistics Agency;
- Personnel—the Director of the DoD Human Resources Activity;
- Public Works—the Chief of the U.S. Army Corps of Engineers;
- Space—the Commander of the U.S. Strategic Command; and
- Transportation—the Commander of the U.S. Transportation Command.⁶

The DoD Changed the Defense Critical Infrastructure Program to a Line of Effort Under the Mission Assurance Program

In 2016, the DoD changed the DCIP to a line of effort under the Mission Assurance Program. According to the 2016 DoD Directive 3020.40, the mission assurance program is designed to sustain programming, resources, functions, and activities supporting responsibilities formerly under the DCIP.⁷ The mission assurance strategic lines of effort include:

- providing DoD policy and guidance;
- performing oversight;

⁶ According to the January 2010 DoD Directive 3020.40, DISLAs were designated DoD officials and their respective defense sector organizations that performed defense infrastructure sector responsibilities in coordination with their respective principal staff assistants. The DISLAs characterized their defense infrastructure sectors to identify functions, systems, interdependencies, and, ultimately, sector task critical assets that support combatant commands, Military Departments, and Defense Agency missions and sector functions.

⁷ DoD Instruction 3020.45, “Mission Assurance (MA) Construct,” August 14, 2018, states that the protection of essential DoD services and infrastructure line of effort are those selective actions under the mission assurance construct directly related to the risk management of essential DoD services and infrastructure. This effort is asset-focused, whereas mission assurance manages all risks to strategic missions, including those from the protection of essential assets and facilities.

- maintaining active partnerships within and across the DoD; and
- engaging with and influencing partners outside the DoD in the interagency, commercial industry, and international entities.

Mission assurance is a risk-management process to protect or ensure the continued function of DoD assets and capabilities.⁸

Counterintelligence Support to Essential DoD Services and Infrastructure

DoD Instruction 5240.19 requires DoD CI components to assign CI support to the DoD sectors and their corresponding DISLAs within the purview of previously established defense sectors of responsibility. DoD Instruction 5240.19 requires that CI activities be conducted in accordance with DoD Directive 3020.40 and DoD Directive 5143.01, and that CI organizations provide comprehensive and timely reporting of foreign intelligence entity threats, incidents, events, and trends to DCIP authorities and the DoD Components.⁹ In 2017, the DoD issued an updated version of DoD Instruction 5240.19. However, the Instruction still referenced sectors and contained CI coverage requirements that were predicated on the existence of DISLAs.

Roles and Responsibilities for Implementing and Overseeing the Defense Critical Infrastructure Line of Effort

DoD Directive 3020.40 assigns roles and responsibilities for the protection of essential DoD services and infrastructure under mission assurance. The directive requires the DoD to continue, under the mission assurance construct and policy, existing efforts to meet national and essential DoD services and infrastructure requirements established by PPD-21. Existing Department-level DCIP policy will remain effective until integrated into, replaced by, or rescinded by mission assurance policy. DoD Components will maintain sufficient resources to meet essential DoD services and infrastructure responsibilities for identifying, assessing, managing, and monitoring risk to critical infrastructure and align associated security, protection, and risk management efforts under a mission assurance construct. DoD Components will sustain and continue to prioritize resources to implement mission assurance decisions in a dynamic threat environment. The Directive assigns DoD-wide critical infrastructure analysis, formerly conducted by the Defense sectors, to parent DoD Components; this includes analysis of DoD and non-DoD networks, assets, and associated dependencies to coordinate and assist other DoD Components' analysis efforts.

⁸ According to DoD Instruction 3020.45, mission assurance synchronizes and integrates aspects of multiple security and protection efforts to manage the risk to the DoD's strategic missions (as shown in Appendix B). DoD guidance prioritizes resources toward addressing the most critical concerns for executing strategic missions.

⁹ DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD[I])," October 24, 2014, with change 1, April 22, 2015. A foreign intelligence entity is any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

Under Secretary of Defense for Policy

According to DoD Directive 3020.40, the Under Secretary of Defense for Policy serves as the Principal Staff Assistant to the Secretary of Defense on mission assurance. The Under Secretary of Defense for Policy coordinates aspects of the DoD's various security, protection, and risk-management programs and efforts directly related to mission execution of mission assurance and ensures that mission assurance is consistent with the all-hazards approach prescribed in PPD-21.

According to DoD Directive 3020.45, the Assistant Secretary of Defense (Homeland Defense and Global Security) is assigned as the lead official for providing policy, guidance, oversight, and resource advocacy for critical infrastructure protection. The Assistant Secretary of Defense (Homeland Defense and Global Security):

- serves as the original classification authority for the protection of essential assets and facilities the lines of effort under mission assurance,
- co-chairs the mission assurance Executive Steering Group with the Director of the Joint Staff, and
- as the principal cyber adviser, aligns principal cyber adviser activities with mission assurance.

Under Secretary of Defense for Intelligence

According to DoD Directive 3020.40, the Under Secretary of Defense for Intelligence (USD[I]) establishes policy and plans to direct and integrate intelligence, CI, and security support to mission assurance activities and, as appropriate, the national DIB Sector Government Coordinating Council. USD(I) establishes policy for the Defense Intelligence Enterprise mission assurance capabilities, priorities, assessments, and investments. In addition, USD(I) oversees Defense Intelligence Enterprise mission assurance activities, in consultation with the Director of National Intelligence.

Director of the Defense Intelligence Agency

According to DoD Instruction 5240.19 the Director of the Defense Intelligence Agency (DIA) plans, integrates, coordinates, directs, and manages intelligence and CI support for the protection of essential assets and facilities line of effort. This includes providing functional management and conducting CI support for the protection of essential assets and facilities line of effort Integrated Management Group.¹⁰ The DIA also coordinates with DoD Components to integrate CI support into overall intelligence support for the protection of DoD critical assets.¹¹

¹⁰ Functional management is the process of planning, organizing, coordinating, controlling, and directing efforts within a structure that groups responsibilities according to the type of work to be performed. Counterintelligence support includes, but is not limited to foreign intelligence, counterespionage, and international terrorist threat awareness briefings, debriefings, reporting, and training activities supporting the DoD Component CI programs, support to the DoD antiterrorism and force protection programs to include participation in CI surveys and vulnerability assessments, support to DoD foreign visitors program, CI inquiries, CI insider threat identification and mitigation efforts, and CI support to research, development, and acquisition to include support to supply chain risk management.

¹¹ The Integrated Management Group is the principal forum for coordinating and sharing essential DoD services and infrastructure line of effort information among the Defense CI Components.

Heads of DoD Components

According to DoD Directive 3020.40, DoD Component Heads are required to assign members of the Senior Executive Service, a general officer, or a flag officer as Component mission assurance lead for integrating mission assurance efforts across the Component. In addition, Component Heads are required to establish and resource an office of primary responsibility for mission assurance that includes, or can coordinate with, the essential assets and facilities line of effort and maintain staffing and resource levels necessary to meet continuing essential DoD asset and facilities responsibilities under mission assurance, including mission assurance process execution and security, protection, and risk-management efforts across the Component.

Finding

DoD Counterintelligence Policy Was Not Aligned With Current Mission Assurance Policy to Protect Essential DoD Services and Infrastructure

USD(I) did not assign responsibilities for CI coverage of essential DoD services and infrastructure previously managed by DISLAs. This occurred because, although DISLA positions were eliminated by DoD Directive 3020.40 in 2016, USD(I) has not yet updated DoD Instruction 5240.19 to assign CI coverage responsibilities that were previously aligned to support DISLAs and their corresponding sectors. As a result, DoD CI support provided through efforts such as threat awareness briefings, CI inquiries, and support to DoD foreign visitors program may not consistently identify CI threats to essential DoD services and infrastructure. Without current and clear guidance, DoD Components cannot provide consistent and comprehensive CI support to essential DoD services and infrastructure.

In addition, from 2015 to 2018, the DIA did not manage the Integrated Management Group to support CI functional management and integration of CI support, as required by DoD Instruction 5240.19. This occurred because, according to DIA officials, attempts to reinvigorate the Integrated Management Group were hampered by limited personnel. As a result, the DoD may not be adequately integrating and coordinating CI support for essential DoD services and infrastructure, which could result in duplicative CI efforts or insufficient CI coverage for these assets.

USD(I) Did Not Assign Responsibilities for Counterintelligence Coverage of Critical Assets and Facilities

USD(I) did not assign responsibilities for CI coverage of critical assets and facilities previously managed by DISLAs. We reviewed DoD policies for the mission assurance program and CI support to the program and found that DoD CI policy does not identify responsibilities for CI coverage of essential DoD services and infrastructure previously managed by DISLAs.

The former DoD sectors and their corresponding DISLAs were a DoD-specific configuration similar to a national-level structure for the protection of essential DoD services and infrastructure. According to DoD Instruction 5240.19, Enclosure 3, paragraph 2, DoD CI Components “will coordinate across defense infrastructure sectors as necessary to ensure that vulnerabilities associated with multiple sectors are adequately addressed,” within the purview of previously

established Defense sectors of responsibility. DoD Instruction 5240.19, Enclosure 2, paragraph 12, requires DoD Component Heads of Defense Infrastructure Sector Lead Agencies to “coordinate with their supporting CI organization to identify and provide CI collection and production requirements.” The structure is outlined in Table 1.

Table. Defense Infrastructure Sectors, Sector Leads, and Support CI Organizations

Defense Infrastructure Sector	Defense Infrastructure Sector Lead Agent (DISLA)	Supporting CI Organizations
DIB	Director, DCMA	Army CI (Lead) DSS (supporting)
Financial Services	Director, Defense Finance and Accounting Service	Naval Criminal Investigative Service (NCIS)
GIG	Director, Defense Information Systems Agency	Army CI
Health Affairs	Assistant Secretary of Defense for Health Affairs	Air Force Office of Special Investigations (AFOSI)
Intelligence	Director, DIA	DIA
Logistics	Director, Defense Logistics Agency	Army CI
Personnel	Director, DoD Human Resources Activity	NCIS
Public Works	Chief, U.S. Army Corps of Engineers	Army CI
Space	Commander, U.S. Strategic Command	AFOSI
Transportation	Commander, U.S. Transportation Command	AFOSI

Source: DoD Instruction 5240.19, “Counterintelligence Support to Defense Critical Infrastructure Program,” January 31, 2014.

However, the Office of the Under Secretary of Defense for Policy changed the DCIP to a line of effort under the mission assurance program in 2016, through the issuance of DoD Directive 3020.40. The 2016 DoD Directive 3020.40 assigns DoD-wide essential DoD services and infrastructure analysis, formerly provided by the DISLAs, to parent DoD Components; however, this change was not reflected by USD(I) in DoD Instruction 5240.19, which caused confusion for DoD Components.

For example, Air Force Office of Special Investigations officials stated that clarity is needed at the USD(I) level with respect to who has the responsibility for critical DoD assets and facilities. Air Force Office of Special Investigations officials cited the Defense Information Systems Agency, the former DISLA for the global information grid sector, with multiple essential assets, as an example of confusion regarding who provides support to those essential assets. Before DISLAs and their associated sectors were eliminated, Army CI was assigned responsibility for this sector; however, it is unclear who should be providing this support since DISLAs no longer exist. The Air Force Office of Special Investigation officials stated that

they did not know who would support assets such as a Tier 1 Task Critical Asset on an Air Force base that may not be mission essential to the Air Force. Air Force officials stated that clarity regarding the responsibilities for CI support is needed to address concerns such as this, especially now that DISLAs and their associated sectors were eliminated and new or relevant responsibilities aligning CI support to critical defense infrastructure have not been assigned in DoD Instruction 5240.19.¹²

USD(I) Has Not Updated Corresponding Essential DoD Services and Infrastructure-Related Counterintelligence Policies

USD(I) has not updated DoD Instruction 5240.19 to reflect the transition of DCIP from a separate program to a line of effort under mission assurance and the corresponding responsibilities, in the absence of Defense sectors. Officials from the Office of USD(I) acknowledged the confusion caused by the lack of an updated Instruction, but as of March 2019, had not updated DoD Instruction 5240.19 to resolve this problem.

According to DoD Directive 3020.40, USD(I) is required to establish policy and plans to direct and integrate intelligence, CI, and security support to mission assurance activities, and coordinate and integrate insider threat policies and efforts with mission assurance. However, because DISLAs and their corresponding Defense sectors were eliminated, the Defense sector support requirements in all applicable DoD policies must be revised to ensure the protection of essential DoD services and infrastructure.

As a result, DoD CI support provided through efforts such as threat awareness briefings, CI inquiries, and support to DoD foreign visitors program may not consistently identify CI threats to essential DoD services and infrastructure. Without current and clear guidance, DoD Components will not be able to provide consistent and comprehensive CI support to essential DoD services and infrastructure. For example, U.S. Transportation Command officials stated that changes to the DCIP (now a line of effort) and the elimination of the role of the DISLAs combined with a lack of updated guidance from USD(I) may undermine CI authorities for protecting essential DoD services and infrastructure.

¹² According to DoD Directive 3020.40, Task Critical Assets, are assets that are of such extraordinary importance that their incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or Office of the Secretary of Defense Components to execute the capability or mission-essential task they support. TCAs are used to identify DCAs. Tier 1 Task Critical Assets are assets of such extraordinary importance that their incapacitation or destruction would have a serious, debilitating effect on the ability of one or more military services or combatant commands the mission-essential task they support.

The DIA Did Not Manage the Integrated Management Group, as Required by DoD Policy

From 2015 to 2018, the DIA did not manage the Integrated Management Group to support CI functional management and integration of CI support, as required by DoD Instruction 5240.19, Enclosure 2, paragraph 3a. According to DoD Instruction 5240.19, as the CI functional manager, the DIA is supposed to plan, integrate, coordinate, direct, synchronize, and manage CI support for the essential DoD services and infrastructure line of effort, including assigning a chair for the Integrated Management Group. DIA officials stated that from 2015 to 2018, attempts to reinvigorate the Integrated Management Group and perform CI functional program management were hampered by limited resources. Prior to this period of inactivity, the DIA was chairing quarterly meetings.

The effort to conduct Integrated Management Group meetings has been inconsistent and incomplete. For example, in a February 5, 2018, oversight report of the DIA, the Office of the DoD Senior Intelligence Oversight Official observed that “DIA has assigned a chair for the Defense Critical Infrastructure Program (DCIP) integrated management group (IMG), but had not hosted a CI Support to DCIP IMG in approximately 2 years, falling short of the intent of DoD Instruction 5240.19.” Moreover, the Office of the DoD Senior Intelligence Oversight Official also observed that DoD Instruction 5240.19 requires the DIA to coordinate with the DoD Components regarding the integration of CI support into overall intelligence support to the DCIP, but this coordination occurs only on an irregular basis.

The absence of a functioning Integrated Management Group continued during the course of our assessment. Although the DIA hired a functional manager in August 2018, and he has conducted two “community of interest” meetings, those meetings were predominantly focused on research, development, and acquisition protection. Although CI support to research, development, and acquisition protection is an important CI support mission, CI support to the essential DoD services and infrastructure line of effort is still a requirement. In order to provide more focused CI support for the protection of essential DoD services and infrastructure, the DIA must be consistent with its CI functional management and collaboration with the CI Enterprise. To meet the requirements of DoD Instruction 5240.19, the DIA should reestablish and appoint a chair to the essential DoD services and infrastructure line of effort Integrated Management Group to enhance CI functional management and integration of CI support to essential DoD services and infrastructure, as required by DoD Instruction 5240.19. In addition to the chair, a deputy should be appointed to ensure continuity.

As a result, the DoD may not be adequately integrating and coordinating CI support for critical DoD assets and facilities, which could result in duplicative CI efforts or insufficient CI coverage for these assets. According to DoD Instructions 5240.16 and 5240.19, effective CI support includes effective coordination that deconflicts coverage and works to improve efficiencies.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, revise all applicable DoD policies to ensure the protection of essential DoD services and infrastructure.

Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence Comments

The Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, agreed with the recommendation, stating that DoD counterintelligence policy will be rewritten by April 2020 to reflect the changes to DoD Directive 3020.40 and DoD Instruction 3020.45, to ensure that counterintelligence responsibilities are aligned to critical asset owners.

Our Response

Comments from the Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, addressed the recommendation; therefore, the recommendation is resolved. The recommendation will remain open until we receive and review the updated policies.

Recommendation 2

We recommend that the Director of the Office of Community Coordination, Defense Intelligence Agency, reestablish and appoint a chair and deputy chair to the Defense Critical Infrastructure Line of Effort Integrated Management Group, to enhance counterintelligence functional management and integration of counterintelligence support to the essential DoD services and infrastructure line of effort, as required by DoD Instruction 5240.19.

Director of the Office of Community Coordination, Defense Intelligence Agency Comments

The Director of the Office of Community Coordination, Defense Intelligence Agency, agreed with the recommendation, stating that an Integrated Management Group chair was appointed in August 2018, and that a volunteer from the Integrated Management Group members will be requested to serve as the deputy chair during the March 28, 2019, Integrated Management Group meeting.

Our Response

Comments from the Director of the Office of Community Coordination, Defense Intelligence Agency, addressed the recommendation; therefore, the recommendation is resolved. The recommendation will remain open until we receive appointment letters for the Integrated Management Group chair and deputy chair, along with the Integrated Management Group meeting minutes.

Appendix A

Scope and Methodology

We conducted this assessment from January 2018 to December 2018, in accordance with the “Quality Standards for Inspection and Evaluation,” published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the assessment to ensure that objectives are met and that we perform the assessment to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions and recommendations.

We received an overview of intelligence, CI, and security support to the essential DoD services and infrastructure line of effort mitigation process, including the National Information Security Policy. We reviewed existing criteria and determined the extent to which the integration of policies governing both mission assurance and essential DoD services and infrastructure line of effort programs and goals are either congruent or divergent. Specifically, we reviewed the following criteria and policies:

Executive Orders and Presidential Policies

- HSPD-7
- PPD-21

DoD Directives

- DoD Directive 3020.40
- DoD Directive 5143.01

DoD Instructions

- DoD Instruction 3020.45
- DoD Instruction 5205.13, “Defense Industrial Base (DIB) Cyber Security (CS) Activities,” January 29, 2010
- DoD Instruction 3020.51
- DoD Instruction 5240.16
- DoD Instruction 5240.19
- DoD Instruction 3020.39

We reviewed the mechanisms for disseminating intelligence and CI findings to appropriate stakeholders, determined whether thresholds or triggers exist in the National Industrial Security Program to generate reporting on essential DoD services and infrastructure line of effort issues. In addition, we evaluated the level of preparedness of personnel assigned to support the essential DoD services and infrastructure line of effort mitigation process.

To obtain additional information we conducted data calls, surveys, and interviews to determine whether existing policies are being successfully implemented. Specifically, we interviewed and obtained information from personnel at the following organizations:

- USD(I)/Defense Intelligence Agency/Defense Intelligence Mission Assurance Office
- Under Secretary of Defense for Policy, Assistant Secretary of Defense (Homeland Defense and Global Security)
- USD(AT&L)/Office of Manufacturing and Industrial Base Policy; DTRA
- Combatant Commands: U.S. Special Operations Command, U.S. Transportation Command, U.S. Central Command, U.S. Northern Command, U.S. Indo-Pacific Command, U.S. European Command, and U.S. Strategic Command
- Military Department CI Organizations/Army G-2, Naval Criminal Investigative Service, and Air Force Office of Special Investigations

Computer-Processed Data

We did not use computer-processed data to perform this assessment.

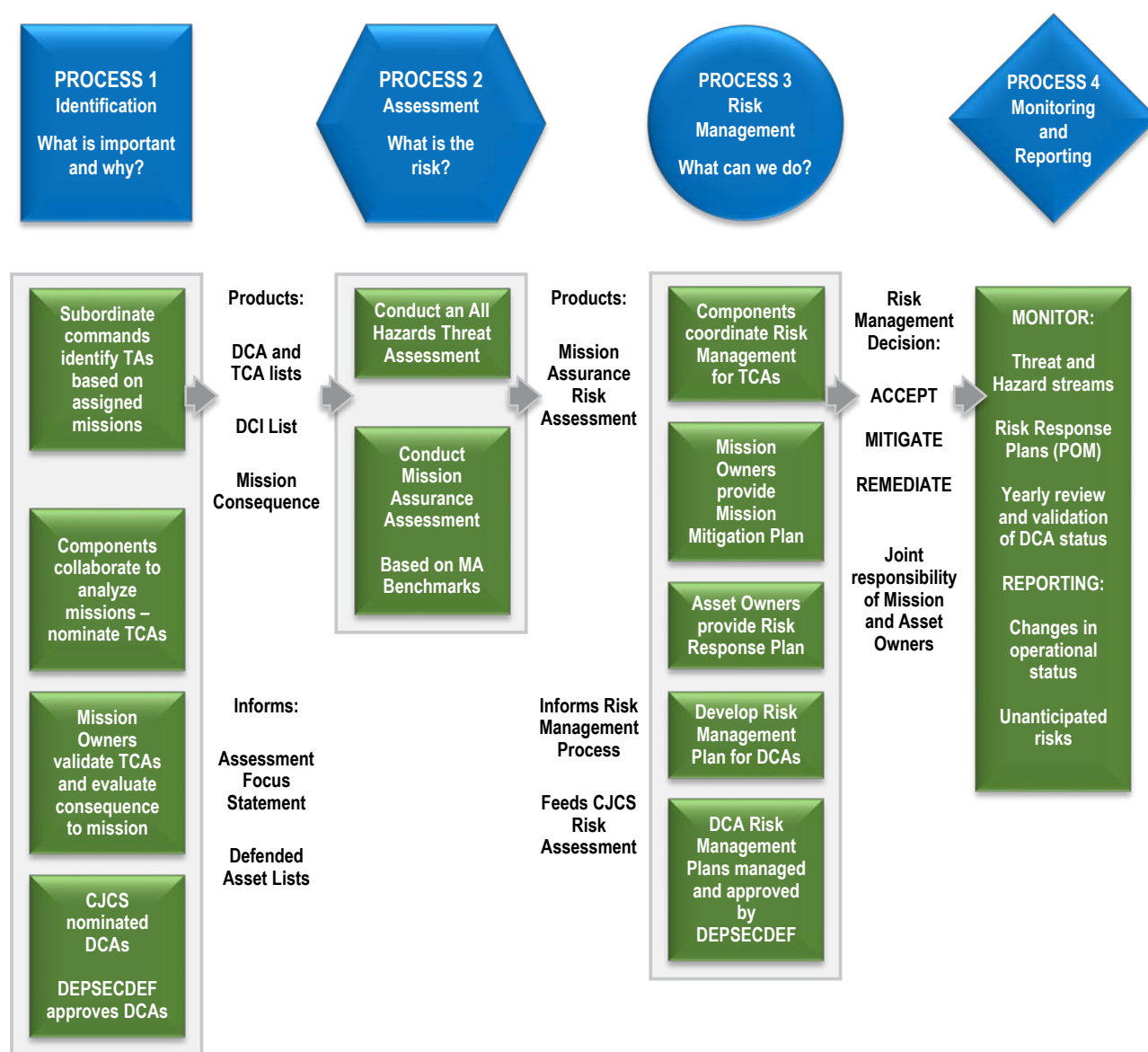
Prior Coverage

During the last 5 years, neither DoD OIG nor GAO issued any reports that addressed issues specific to this assessment. Unrestricted DoD OIG reports are at <http://www.dodig.mil/reports.html/>.

Appendix B

Mission Assurance Construct Process Chart

According to DoD Instruction 3020.45, Mission Assurance prioritizes DoD efforts and resources to address the most critical strategic mission execution concerns for protecting the essential DoD services and infrastructure. The Mission Assurance Construct's four processes are identification, assessment, risk management, and monitoring. Their relationship to one another and products are illustrated below.



Management Comments

Chief of Staff, Office of the Under Secretary of Defense for Intelligence



INTELLIGENCE

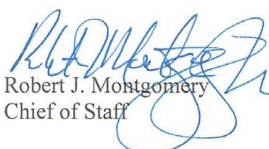
OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

MAR 15 2019

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: MR. INGRAM, PROJECT MANAGER, OFFICE OF THE
DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND
SPECIAL PROGRAM ASSESSMENTS)

SUBJECT: Draft, "Evaluation of DoD Component Responsibilities for Counterintelligence
Support for the Protection of Defense Critical Infrastructure"

I concur with the final draft Report as written. We greatly appreciate your knowledge
and engagement during this effort, and we will work with our Policy and Counterintelligence
mission partners in implementing your recommendations.


Robert J. Montgomery
Chief of Staff

cc:
Deputy Director, Counterintelligence and Security, OUSD(I)
Director of Mission Assurance, OUSD(P)
Chief, DoD Infrastructure Threats Division Americas Regional Center, DIA



Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

March 13, 2019

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
(ATTN: MR. DAVID INGRAM)

SUBJECT: Evaluation of DoD Component Responsibilities for Counterintelligence Support for
the Protection of Defense Critical Infrastructure (Project No. D2018-DISPA2-
0096.000)

In response to your February 28, 2019, request for review of the subject document, we
concur and provide the attached comment. My point of contact is Mr. Richard Morefield at



Matthew Blake
Director, Counterintelligence & Law
Enforcement

Attachment:
As stated



Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence (cont'd)

RECOMMENDATION 1: We recommend that the Director for Defense Intelligence (Intelligence and Security), Office of the Under Secretary of Defense for Intelligence, revise DoD Instruction 5240.19 to align DoD Components with corresponding counterintelligence support organizations for the protection of essential DoD services and infrastructure.

RESPONSE: Concur. Recent changes in DoD policies (specifically DoD Directive 3020.40 and DoD Instruction 3020.45) changed the design of the Defense Critical Infrastructure Program (DCIP) and renamed it DoD Mission Assurance (MA). These changes also removed the Defense Infrastructure Sector Leads (DISLA) from the original DCIP organizational structure. Under the current DoDI 5240.19, Counterintelligence Support to Defense Critical Infrastructure Program, specific DoD counterintelligence organizations were aligned to support specific DCIP sectors and the DISLAs. The new DoD Mission Assurance guidance structure assigns DCI protection responsibilities to the asset owner. DoD CI guidance will be re-written to reflect these changes and ensure that CI responsibilities are aligned to the asset owner. We are discussing whether to re-write DoD 5240.19, add a section regarding CI Support to Mission Assurance to DoD 5240.02, or incorporate CI language into DoDI 3020.51 Intelligence Support to the Defense Critical Infrastructure Program. We will endeavor to have the new guidance published by April 2020.

Director of the Office of Community Coordination, Defense Intelligence Agency



DEFENSE INTELLIGENCE AGENCY

U-10,325-19/CCO

March 7, 2019

(U) Subject: DoD Office of Inspector General Evaluation of DoD Component Responsibilities for Counterintelligence Support for the Protection of Defense Critical Infrastructure (Project No. D2018-DISPA2-0096.000), dated 28 February 2019.

(U) This paper responds to Department of Defense Office (DoD) Office of Inspector General Evaluation of DoD Component Responsibilities for Counterintelligence Support for the Protection of Defense Critical Infrastructure

(U) In response to your February 29, 2019 request for review of the subject document, we concur and provide the following comments.

(U) Regarding Finding #2, the Defense Intelligence Agency (DIA) appointed a GG-14, CI Special Agent to serve as the CI support to Defense Critical Infrastructure Program (DCIP) Functional Manager (FM) and Chair of the DCIP Integrated Management Group (IMG) in August 2018. DIA has a dedicated effort that provides functional management and oversight for enterprise-wide coordination of CI resources on critical infrastructure who has consistently chaired quarterly DCIP IMG meetings as required by DoD Instruction 5240.19. The next IMG is scheduled for 28 March 2019.

(U) Regarding the recommendation to also appoint the Deputy Chair of the DCI IMG from the DIA staff, DIA lacks the resources to serve as both the Chairman and Deputy Chairman of the IMG. Instead, DIA will solicit a volunteer from a member of the IMG to serve as the Deputy during the next IMG (28 March 2019).

(U) Prepared by: [REDACTED]

A handwritten signature in black ink, appearing to read "B. E. Jackson".

Brian E. Jackson
CI Division, Community Coordination Office
Defense Intelligence Agency

Committed to Excellence in Defense of the Nation

Acronyms and Abbreviations

CI	Counterintelligence
DCIP	Defense Critical Infrastructure Program
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DIE	Defense Intelligence Enterprise
DISLA	Defense Infrastructure Sector Lead Agent
HSPD	Homeland Security Presidential Directive
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OUSD(P)	Office of the Under Secretary of Defense for Policy
PPD	Presidential Policy Directive
USD(I)	Under Secretary of Defense for Intelligence

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

**For more information about DoD OIG
reports or activities, please contact us:**

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

