Department of Homeland Security

Office of Inspector General

Domestic Nuclear Detection Office Has Taken Steps To Address Insider Threat, but Challenges Remain

OIG-14-113

July 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

July 21, 2014

MEMORANDUM FOR: The Honorable Dr. Huban Gowadia
Director
Domestic Nuclear Detection Office

FROM: John Roth
Inspector General

SUBJECT: *Domestic Nuclear Detection Office Has Taken Steps To Address Insider Threat, but Challenges Remain*

Attached for your information is our final report, *Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, but Challenges Remain.* We incorporated the formal comments from DNDO in the final report.

The report contains five recommendations aimed at improving DNDO's insider threat posture. Your office concurred with all recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, all of the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Richard Harsche, Acting Assistant Inspector General for Information Technology Audits, at (202) 254-5448.

Table of Contents

Appendixes

Abbreviations

CERT	Computer Emergency Response Team
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
I&A	Office of Intelligence and Analysis
ISVM	Information Systems Vulnerability Management
IT	information technology
ITTF	Insider Threat Task Force
JACCIS	Joint Analysis Center Collaborative Information System
LAN-A	Local Area Network-A
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OIG	Office of Inspector General
PII	personally identifiable information
SOC	Security Operations Center

Executive Summary

We reviewed the efforts of the Domestic Nuclear Detection Office (DNDO) to address the risk posed by trusted insiders. Our objective was to assess DNDO's progress toward protecting its information technology assets from threats posed by its employees, especially those with trusted or elevated access to sensitive, but unclassified information systems or data.

Steps are underway to address and mitigate the insider risk at DNDO. Specifically, the Department of Homeland Security (DHS) Acting Under Secretary of Intelligence and Analysis established an Insider Threat Task Force to develop a program to address the risk of insider threats for DHS, including DNDO. In addition, the DHS Office of Intelligence and Analysis has detailed a counterintelligence officer to DNDO to help mitigate espionage-related insider risks. The DHS Office of Intelligence and Analysis routinely briefs DNDO on counterintelligence awareness, including insider threat indicators. In addition, DNDO provides security awareness training to its employees and contractors regarding security-related topics that could help prevent or detect the insider risk. In September 2013, the DHS Office of the Chief Security Officer began a comprehensive vulnerability assessment of DNDO assets, which includes identifying insider risks and vulnerabilities. The DHS Security Operations Center monitors DNDO information systems and networks to respond to potential insider based incidents. Finally, the DHS Special Security Programs Division handles and investigates security incidents, including those types attributed to malicious insiders.

Additional steps to address the insider risk at DNDO are required. Specifically, DNDO needs to implement insider threat procedures, upon receipt of policy issued by the DHS Office of the Chief Information Officer (OCIO) that defines roles and responsibilities for addressing insider risks to unclassified networks and systems. DNDO also needs to provide documentation that clearly shows the effectiveness of controls or processes in place to detect and respond to unauthorized data exfiltration from DNDO unclassified information technology assets via email services provided by the DHS OCIO.

DNDO can strengthen processes and controls for its own technology infrastructure. They can disable portable media ports on controlled information technology assets where there is no legitimate business need. DNDO can apply critical security patches to these assets and perform periodic security assessments of controlled sites to identify any indication of unauthorized wireless devices or connections to DHS networks.

We are making five recommendations that, if implemented, should strengthen DNDO's security posture against the risk posed by trusted insiders.

Background

The *National Security Presidential Directive NSPD-43/Homeland Security Presidential Directive HSPD-14* established the Domestic Nuclear Detection Office in April 2005. This improved the Nation's ability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the United States. To accomplish this mission, DNDO collaborates with Federal, State, local, tribal, and international governments and the private sector. DNDO also relies on expertise from other DHS Components such as the U.S. Coast Guard, U.S. Customs and Border Protection, and the Transportation Security Administration, as well as interagency partners from the Department of Defense, Department of Energy, Federal Bureau of Investigation, and Nuclear Regulatory Commission. As of June 2013, DNDO had 122 Federal employees and 159 onsite contractors, most of whom are located in the Washington, DC area. DNDO received approximately $303 million in funding in fiscal year 2013.

Presidential Directives and Federal laws require DNDO to support and enhance the effective sharing and use of nuclear and radiological detection information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments. DNDO enhances and maintains continuous awareness through analysis of information from all mission-related detection systems. DNDO primarily conducts these functions through the Joint Analysis Center and its supporting Joint Analysis Center Collaborative Information System (JACCIS).

DNDO relies on the DHS Office of the Chief Information Officer for most of its information technology (IT) and infrastructure support services such as enterprise desktop, file, email, port, and network services (e.g., Local Area Network A, Email-as-a-Service, and Homeland Security Information Network). Similarly, DNDO uses other systems, such as those of the Office of Procurement Operations, the Science and Technology Directorate, and the U.S. Coast Guard, for time and attendance, business collaboration, program planning, procurement, and budget and finance support. DNDO uses the DHS Office of the Chief Human Capital Officer for human resource services and the DHS Office of the Chief Security Officer (OCSO) for security and personnel vetting services.

Trusted insiders are typically given unfettered or elevated access to mission-critical assets, including personnel, facilities, information, equipment, networks, or systems. Potential threats can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information. Trusted insiders may also be aware of weaknesses in organizational policies and procedures, as well as physical and technical vulnerabilities in computer networks and information systems. This

institutional knowledge poses a continual risk to the organization. In the wrong hands, insiders use it to facilitate malicious attacks on their own or collude with external attackers to carry out such attacks.

According to DNDO officials, a malicious insider could do the most harm to a DNDO system by:

- disrupting communications and limiting timely notification, analysis, and reporting of detection of radiological and nuclear materials out of regulatory control;
- reducing or denying access to data needed to analyze and develop situational awareness; and
- diminishing accuracy and completeness of detection event data.

In addition, unauthorized disclosure of sensitive information could adversely affect the security of DNDO's information systems, assets, resources, employees, and the general public. In the case of DNDO, an internal breach by a trusted employee could impact its ability to respond to nuclear detection alarms and coordinate a U.S. Government response to a nuclear incident. As a result, the office must be constantly aware of adversaries, especially those with the expertise and means to create opportunities for insider attacks.

Requirements and Best Practices for Addressing Insider Risks

Issued in October 2011, *Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, requires agencies to implement a threat detection program consistent with guidance and standards developed by a government-wide insider threat task force. DHS, in coordination with DNDO, will be responsible for implementing this program consistent with the task force's guidance. The November 2012 *Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* promotes the development of effective insider threat programs within the U.S. Government.

National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, issued in April 2013, includes new requirements for agencies to address the risk posed by the insider threat. Federal agencies had up to 1 year from April 2013 to comply with this requirement. According to NIST, the standards and guidelines that

apply to insider threat programs in classified environments are effective to improve the security of controlled unclassified information in non-national security systems.

Since 2001, the Computer Emergency Response Team (CERT) Insider Threat Center of the Software Engineering Institute at Carnegie Mellon University has researched and gathered data about malicious insider acts, including IT sabotage, fraud, and theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures. CERT has researched approximately 400 insider threat cases, including fraud, sabotage, and theft of intellectual property; all prosecuted within the United States.

CERT's research resulted in developing best practices that provide a framework for establishing an insider threat program within an organization, including Federal agencies. In addition, CERT devised a list of defensive measures that could help detect or prevent insider attacks. CERT recommends that organizations:

- include insider threat as part of an enterprise-wide risk assessment;
- conduct a security awareness campaign to ensure that the insider threat is understood across the organization;
- develop and clearly define organizational policies relevant to the insider threat, enforcing those policies consistently and fairly; and
- secure both the physical and electronic environment, including account and password management, separation of duties, controls for the software development process, change controls, remote access, and privileged user accounts, especially those used by system administrators.

Results of Audit

Steps Taken To Mitigate the Insider Risk at DNDO

Steps are underway to address and mitigate the insider risk at DNDO. Specifically, the DHS Acting Under Secretary of Intelligence and Analysis (I&A) established an Insider Threat Task Force (ITTF) to develop a program to address the risk of insider threats for DHS, including DNDO. In addition, the DHS I&A has detailed a counterintelligence officer to DNDO to help mitigate espionage-related insider risks. The DHS I&A routinely briefs DNDO on counterintelligence awareness, including insider threat indicators. In addition, DNDO provides security awareness training to its employees and contractors that include security-related topics that could help prevent or detect the insider risk.

In September 2013, the DHS OCSO began a comprehensive vulnerability assessment of DNDO assets, which includes identifying insider risks and vulnerabilities. The DHS Security Operations Center (SOC) monitors DNDO information systems and networks to respond to potential insider based incidents. Finally, the DHS Special Security Programs Division handles and investigates security incidents, including those types attributed to malicious insiders.

DHS Insider Threat Task Force

On August 10, 2012, the DHS Secretary delegated overall responsibility for developing a DHS-wide Insider Threat Program to the I&A Under Secretary. On January 16, 2013, the Acting Under Secretary of I&A created ITTF to manage, account for, and oversee DHS' classified information safeguarding efforts, and monitor all cleared DHS personnel for insider threat, including DNDO's efforts. ITTF's goals are to:

- monitor user activity on computer networks used by cleared DHS personnel and contractors to detect activity indicative of insider threat behavior;
- maintain an analysis and response capability to electronically gather, integrate, review, assess, and respond to information derived from counterintelligence, internal affairs, security, law enforcement, human resources, antiterrorism, user activity monitoring, or other information sources, as appropriate;
- serve as the DHS clearinghouse for the aggregation and integration of all data on insider threats at DHS;

- gather and integrate available information to conduct a preliminary review of any potential insider threat issues; when a potential threat is identified, take appropriate action by referring the matter;
- oversee departmental employee training on insider threat awareness, specifically the inherent risk posed by the insiders to classified information, operations, and personnel;
- maintain an internal DHS network site, accessible to all DHS personnel, for insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements, and procedures; and provide an electronic means to report suspicious behaviors to the ITTF;
- identify policies and procedures required to develop the DHS Insider Threat Program; and
- keep ITTF standard operating procedures current and work with the Office of the General Counsel and the Privacy Office to maintain the integrity DHS employees' civil rights, civil liberties, and privacy concerns.

In October 2013, ITTF established a DHS-wide intranet website that DNDO can access. The site includes additional details about the DHS Insider Threat Program, resources for insider threat awareness materials, and an email address to report suspicious activities.

DHS Office of Intelligence and Analysis Detailed Employee

In September 2012, I&A detailed a counterintelligence officer to support DNDO leadership and personnel, and to provide foreign travel pre-briefings and debriefings, awareness training, foreign visitor/contact reviews, and counterintelligence threat reporting, all aimed at mitigating espionage-related insider threats.

The detailee is the designated point of contact for any insider threat issues specific to DNDO. As of May 2013, the detailee began providing classified briefings to the DNDO Director and Assistant Directors on specific foreign intelligence threats to DNDO personnel and programs. In addition, the I&A detailee provides routine counterintelligence awareness briefings to DNDO personnel during orientation seminars for new employees (Federal employees and contractors), at recurring security awareness training sessions, and during pre-briefings of personnel with foreign travel and foreign contact. The briefings include information on insider threat indicators. The detailee also works with DNDO Program Managers, security, IT, and other key personnel to identify critical DNDO information and the risk posed by such entities.

Security and Awareness Training

The DNDO Security Office provides annual security training to DNDO employees, contractors, and detailees that could increase their ability to identify and prevent insider risks. Specifically, this training includes instruction on badging and visitor control (including foreign visitors), security requirements for conducting classified meetings, document storage and control, transmission of information security, classification management, information system security, operations security, critical information protection, security classification guides, counterintelligence awareness, and active shooter preparedness.[1]

ITTF is in the final stages of deploying a department-wide, computer-based training module that meets the minimum standards of the *Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*. ITTF anticipates deploying this training module to DHS employees and contractors, including DNDO, during early 2014. In addition, the DHS Chief Learning Officer plans to include a 30-minute insider threat awareness training module in annual mandatory training for all DHS employees and for contractors with a secret or higher security clearance.

Vulnerability Assessment

In September 2013, the DHS OCSO performed a Multiple Disciplinary Vulnerability Assessment at DNDO Headquarters. This assessment looks at identifying insider threat risks and vulnerabilities from an operational, technical, and physical perspective.

The Multiple Vulnerability Disciplinary Assessment included:

- interviews with DNDO employees to identify and confirm potential security vulnerabilities;
- requests for information on security programs;
- querying web logging for foreign interest in DNDO programs or the presence of search queries for sensitive DNDO programs;

[1] DHS provides courses, materials, and workshops to better prepare employees to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.

- open source analysis for indications of threat data or the presence of any DNDO-sensitive material present in the public domain;
- tabletop exercises on security incident response and security anomalies;
- review of contracts for security-related language (i.e., reporting procedures);
- review of foreign visitor data for trends related to known threats to DHS information;
- analysis to identify foreign intelligence threats to DNDO information;
- physical security assessments of the entire DNDO environment to determine vulnerabilities that could be breached; and
- assessments to identify vulnerabilities an employee could exploit from inside DNDO, personnel, physical, or information systems-related vulnerabilities.

At its discretion, the DHS OSCO conducts Multiple Disciplinary Vulnerability Assessments of DNDO. Due to the sensitivity of their mission, DNDO needs to schedule these efforts on a regular basis. During this review, DHS OSCO indicated plans to present a comprehensive report of the findings to DNDO management in 2014.

DHS Security Operations Center

The DHS SOC centrally identifies, monitors, and responds to potential insider threats and incidents on DHS information systems and networks, including those of DNDO. The SOC monitors computer networks and information systems daily to identify potential insider threat activity. According to CERT research, monitoring and logging employees' behavior while they are using government-issued computers and network resources helps to identify suspicious insider activity before a serious breach of security can occur. SOC activities include analyzing computer system security event logs and responding to computer security incidents, as needed.

In addition, the SOC, in coordination with the DHS Information Technology Services Office, has programs and processes designed to detect unauthorized insider threat actions that, if left unchecked, could threaten DNDO's mission. These programs and processes include:

- monitoring DHS external Internet connections using data loss prevention technology to facilitate identifying sensitive information exfiltration;

- monitoring secure remote access connections to DNDO IT assets to detect unusual authentication attempts from external DHS sites to respond to these attempts;
- blocking DNDO personnel from connecting unauthorized portable media devices to the DHS unclassified network;
- establishing a program to help ensure only authorized modifications to IT systems are implemented;
- separating application developers' duties to ensure that one individual cannot modify code and enter the code directly into production systems; and
- establishing the Computer Security Incident Response Center as a single location for employees to report computer-related security incidents. This includes suspicious or anomalous events or actions. The SOC in turn reports such incidents to the United States Computer Emergency Readiness Team (US-CERT) and other DHS stakeholders.

Security Incident Handling and Insider Threat Investigations

In May 2003, on behalf of DNDO, DHS established the Special Security Programs Division in the DHS OCSO. This division's responsibilities include receiving and processing allegations of misconduct and other reported incidents involving personnel and contractors. Allegations can include potential insider threat incidents occurring on or against DNDO information systems or networks. Additionally, DNDO employees can report potential or actual issues of employee misconduct to the Special Security Program Division for further investigation.

The division also serves as the conduit to the DHS Office of Inspector General (OIG). By statute, OIG has the lead investigative role and retains the "right of first refusal" on all allegations of misconduct involving DHS personnel and contractors.[2] OIG accepts certain allegations for investigation and refers those not accepted back to the division for investigation, fact-finding, or immediate action. For each referral, the division assigns an investigator from the OCSO investigation branch to conduct the investigation of significant violations and incidents.

[2] The *Inspector General Act of 1978* (Public Law 95−452), as amended, assigned to OIG the dominant role in investigating criminal and noncriminal allegations against departmental employees, contractors, and grantees. "Right of first refusal" is used primarily by investigators to describe the process, but the act is the origination and basis for that process.

Challenges Remain in Addressing the Insider Risk

Additional steps to address the insider risk at DNDO are required. Specifically, DNDO needs to implement insider threat procedures, upon receipt of policy issued by the DHS OCIO that defines roles and responsibilities for addressing insider risks to unclassified networks and systems. DNDO also needs to provide documentation that clearly shows the effectiveness of controls or processes in place to detect and respond to unauthorized data exfiltration from DNDO unclassified IT assets via email services provided by the DHS OCIO.

DNDO can strengthen processes and controls for its own technology infrastructure. For example, DNDO can disable portable media ports on their controlled information technology assets where there is no legitimate business need. DNDO can also apply critical security patches to these assets and perform periodic security assessments of their controlled sites to identify unauthorized wireless devices or connections to DHS networks.

Insider Threat Policies and Procedures

DNDO has not implemented procedures that define roles and responsibilities for addressing insider risks to unclassified networks and systems. These procedures should integrate the requirements, standards, and guidance provided by the administration, DHS, and NIST.[3] According to DNDO, the DHS OCIO is responsible for developing such policy.

NIST recommends that organizations develop clearly defined policies for addressing insider risks and enforce these policies consistently for maximum effectiveness. Further, CERT recommends that organizations formalize a capability that can monitor and respond to insider risks. This would require establishing policies and procedures for addressing insider threats that encompass human resources, legal, physical and personnel security, management, and IT. From an insider risk management perspective, CERT recommends an organization implement policies that address areas, such as:

[3] Requirements, standards, and guidance referred to include: Executive Order 13587 – *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*; December 2012 draft of the *DHS Insider Threat Policy and Minimum Standards*; and NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

- acceptable use of IT resources;
- monitoring of IT resources;
- protecting intellectual property;
- managing employee use of social media; and
- employee resignations and separations.

According to DNDO, DHS OCIO has developed policies related to four of these five areas, with the exception of protecting intellectual property. Upon receipt of these policies from DHS OCIO, DNDO should implement procedures that define roles and responsibilities for addressing insider risks to unclassified networks and systems. Without such procedures, it can be difficult to discipline, terminate, or prosecute employees who engage in insider threat activity. Further, DNDO employees may not have the guidance and understanding of their role and responsibilities for mitigating the insider risk on a consistent basis.

Data Exfiltration

DHS Headquarters is responsible for monitoring DNDO information systems and information against unauthorized data exfiltration by its employees, including through the use of email applications. However, DHS Headquarters has not fully implemented mechanisms and processes to monitor for and detect instances of unauthorized exfiltration of sensitive information via email accounts. Sensitive or mission-critical information in the wrong hands could have adverse effects on DNDO employees, resources, business partners, or the general public.

OIG technical testing and onsite system inspection confirmed that sensitive information could be sent from a government-issued computer to the Internet using government and personal email accounts (e.g., Yahoo and Gmail) without detection.

We notified the DNDO Chief Information Officer about these vulnerabilities. Subsequently, the Local Area Network-A (LAN-A) Information System Security Manager blocked personal email websites (Gmail, Hotmail, Yahoo) from the DNDO LAN-A network on October 22, 2013.

Portable Media Devices

DHS Headquarters is not currently using technology to monitor and alert security personnel to potentially unusual employee behavior, such as removing large amounts of sensitive information from DNDO information systems using an

authorized portable media device. Unauthorized removal or theft of sensitive information such as intellectual property is a constant threat, and due to the DNDO mission, could negatively impact DNDO employees, resources, business partners, or the general public.

Continuous monitoring of information system events (e.g., login sessions, file access, etc.) significantly reduces the likelihood that an employee can steal or destroy mission critical or sensitive information. The risk of employees becoming insider threats increases when given extensive knowledge of the inner workings of the organization coupled with authorized access to information systems.

DHS Headquarters limits the type and brand of portable media devices (for example, thumb drives) that can connect to its information systems. They do this through a software utility configured to allow specific types and brands of portable devices. According to the DHS OCIO, DHS HQ is not actively monitoring portable media device usage due to the large number of false positives and the time and effort needed to investigate each event.

According to DNDO officials, they would benefit from timely alerts regarding employees that engage in potentially suspicious behavior such as removing large amounts of data using portable media devices connected to DNDO assets. Without active monitoring of real-time system events that includes auditing of system logs, DNDO is limited in its ability to detect and respond in a timely and effective manner to this persistent threat.

Critical Security Patches

Through our technical security assessments of DNDO information systems, we determined DNDO did not implement certain critical security patches. For example, we identified an IT information system used by DNDO that did not have a security patch to protect against known vulnerabilities in JAVA, a platform that runs system programs and web-based applications. For information systems (e.g., JACCIS) under their direct control, DNDO needs to install critical security patches on a continual basis in accordance with DHS security policy.

According to the *DHS 4300A Sensitive Systems Handbook*, components are to reduce system vulnerabilities by testing for vulnerabilities, promptly installing patches, and eliminating or disabling unnecessary services.

CERT case studies have shown that malicious insiders have exploited known technical security vulnerabilities to obtain system access and carry out an attack. An inside attacker with knowledge of these vulnerabilities would likely be able to attack more quickly and with fewer restrictions. Thus, by not implementing these patches, DNDO the likelihood that an attacker could exploit vulnerabilities increases, which could in turn compromise the confidentiality, integrity, or availability of an IT system.

Wireless Scans

DNDO had not performed wireless security scans of its facilities to identify non-DHS wireless access points operating within close proximity to its networks, identify DNDO issued laptop or desktop computers not configured to connect to those access points, or detect non-authorized wireless access points connected to its networks.

DHS 4300A Sensitive Systems Handbook requires components to perform periodic scans to identify vulnerabilities and take corrective actions. Conducting these scans significantly increases the likelihood of detecting or preventing inappropriate or malicious activity by an insider. For example, an insider could connect to a non-DNDO wireless network and remove sensitive information to an unauthorized location outside of the DHS network. Or, an individual could install an unauthorized wireless access (entry) point on a DNDO network to allow for a number of malicious cyber-attacks against DNDO information or information systems.

Without an established process to perform regular wireless vulnerability and security scans, DNDO cannot effectively evaluate wireless security risks affecting its operations on a regular basis or take timely and necessary corrective actions.

Recommendations

We recommend that the Director for DNDO:

Recommendation #1:

Implement insider threat procedures, upon receipt of policy issued by DHS OCIO that defines roles and responsibilities for addressing insider risks to unclassified networks and systems.

Recommendation #2:

Provide documentation that clearly shows the effectiveness of controls or processes in place to detect and respond to unauthorized data exfiltration from DNDO unclassified IT assets via email services provided by OCIO.

Recommendation #3:

Disable portable media ports on unclassified IT devices under direct DNDO control where no business need exists to have them enabled.

Recommendation #4:

Apply critical security patches on DNDO IT assets in accordance with DHS security policy.

Recommendation #5:

Perform periodic security assessments of DNDO sites to identify unauthorized wireless devices or connections.

Management Comments and OIG Analysis

We obtained written comments on a draft report from the Director for DNDO. We have included a copy of the comments, in its entirety, in appendix B. DNDO concurred with all of the recommendations.

DNDO Comments on Recommendation #1

DNDO concurs with recommendation #1. DNDO stated that DNDO OCIO and DHS OCIO agree that insider threat policies and procedures that define roles and responsibilities, from network to user level, are fundamental for addressing insider risks to unclassified networks and systems. Accordingly, DHS OCIO has developed related policy documented in DHS Sensitive Systems Policy Directive 4300A, that meets all of the requirements recommended by the United States Computer Emergency Readiness Team (US-CERT), except for protection of intellectual property. The relevant statements can be found in the following sections of this directive:

- Acceptable use of IT resources: Section 4.1.2, "Rules of Behavior" and Section 4.8.5, "Personal Use of Government Office Equipment and DHS Systems/Computers";
- Monitoring of IT resources: Section 4.1.2, "Rules of Behavior," Section 4.8.5, "Personal Use of Government Office Equipment and DHS Systems/Computers," and Section 5.2.3, "Warning Banner";
- Managing employees use of social media: Section 3.16, "Social Media"; and
- Employee resignations and separations: Section 4.1.6, "Separation from Duty".

DNDO will document its implementation of the existing policy by December 31, 2014. No later than December 31, 2014, DHS OCIO will: (1) develop and incorporate policy in Directive 4300A addressing the protection of intellectual property and (2) work with DNDO OCIO to identify any additional insider threat-related requirements beyond Directive 4300A with which DNDO needs to comply. DNDO OCIO will then expeditiously document its implementation of the

revised Directive 4300A and the additional requirements, if any. The estimated completion date for this recommendation is December 31, 2014.

OIG Analysis

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and unresolved until DNDO provides documentation to support that the planned corrective actions are completed.

DNDO Comments on Recommendation #2

DNDO concurs with recommendation #2. DNDO stated that DNDO will coordinate with DHS OCIO to ensure the latter implements the requirements security controls or processes, and provides DNDO documentation of their effectiveness. DHS OCIO already has a data loss prevention solution at the gateway that monitors emails for extrusion, which is monitored for anomalous traffic, that, when identified, results in actions being taken, as appropriate. A mandated requirement to detect and respond to unauthorized data exfiltration via email applications on unclassified networks, however, has not yet been codified in either Federal or agency policy, consequently, funding for implementing a technical means to satisfy such a requirement and the full intent of this recommendation does not exist at this time.

DNDO OCIO has discussed and coordinated with DHS OCIO about this matter, which is beyond DNDO's authority to address on its own. DHS OCIO advised that once guidance and funding is in place, they will provide additional architecture solutions and implementation, as appropriate. Given the action taken to address this recommendation and the fact that additional action are beyond DNDO's authority, DNDO requests that OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and unresolved until DNDO provides the

documentation to support that the planned corrective actions are completed. DNDO should provide OIG documentation that clearly states the effectiveness of controls or processes in place to detect and respond to unauthorized data exfiltration from DNDO unclassified IT assets via email services provided by OCIO.

DNDO Comments on Recommendation #3

DNDO concurs with recommendation #3. DNDO stated that DNDO OCIO agrees that the use or portable media devices and pose a potential threat, and, as such, will implement appropriate controls and processes on portable media ports for systems owned and registered by DNDO. For systems where ports remain active in order to satisfy business requirement, documentation will be provided explaining implementation and operation of risk mitigating process controls. The estimated completion date for this recommendation is December 31, 2014.

OIG Analysis

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and unresolved until DNDO provides documentation to support that the planned corrective actions are completed.

DNDO Comments on Recommendation #4

DNDO concurs with recommendation #4. DNDO stated that DHS OCIO and DNDO OCIO recognize that DHS information might be subject to unauthorized access and disclosure through exploit of vulnerabilities potentially discoverable in selected DHS information technology assets. DHS OCIO and DNDO OCIO aggressively and regularly apply security patches to their information systems, per the Information System Vulnerability Management (ISVM) process. DHS OCIO ensures that all DHS OCIO information technology assets, which include assets used by DNDO, have the latest software security upgrades as directed by US-CERT or requests waivers or exceptions for ISVM's necessary of legacy systems that cannot be upgraded within the time listed for compliance by US-

CERT. Accordingly, DNDO requests that OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and unresolved until DNDO provides documentation to support that the planned corrective actions are completed or provides exceptions/waivers for not applying critical security patches on DNDO IT assets.

DNDO Comments on Recommendation #5

DNDO concurs with recommendation #5. DNDO stated that DNDO OCIO and DHS OCIO agree that periodic wireless assessments of DHS HQ sites, which include those used by DNDO, to identify unauthorized connections to DHS information technology assets, such as an external network, is a helpful tool in managing insider threat risk. Accordingly, DHS OCIO has already taken steps to implement technology and processes that will enable such assessments. Specifically, the LAN A Information System Security Officer conducts periodic wireless assessments of DHS HQ locations within the National Capital Region on a regular basis for unauthorized wireless connections. Further, DNDO and DHS OCIO will formalize the periodicity of the assessments conducted at DNDO. Any connection suspected of an insider threat is evaluated to determine if it is connected to a DHS IT asset, and if so, it is disconnected and reported per DHS policy, as appropriate. Accordingly, DNDO requests that OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and unresolved until DNDO provides documentation to support that the planned corrective actions are completed by providing the OIG with a formalized periodic schedule on when the wireless assessments will be conducted at DNDO.

Appendix A
Objectives, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

Our objective was to assess the progress made towards protecting the Department's IT assets from the threat posed by its employees, especially those with trusted or elevated access to these assets. During the audit, we assessed DNDO's:

- insider threat management process;
- ability of selected employees to monitor and report suspicious employee behavior;
- insider threat security policies;
- insider threat security training and awareness; and
- selected unclassified information systems critical to the mission of DNDO.

We reviewed DNDO and DHS policies, procedures, management plans, and wireless network security policies and documents. In addition, the assessment team reviewed system and security logs for unauthorized devices and wireless activities. We interviewed selected DNDO personnel and management officials stationed at the DNDO Headquarters offices in Washington, DC.

Technical fieldwork performed at selected locations included the following activities:

- Physical and Visual Inspection Check: We inspected offices and designated IT areas to determine how effectively information systems and workstations were logically and physically protected from the threat of exposed sensitive information being accessed or obtained by a malicious insider. Our inspection included checking for exposed or unattended user accounts (e.g., user names and password information), unprotected personally identifiable information (PII), sensitive or classified DNDO information, and the presence of locking mechanisms for IT assets in accordance with Department policy.

- Unauthorized Portable Electronic Devices Testing: We selected and tested a sample of information systems and workstations to determine if sensitive information could

be exfiltrated from the DNDO/DHS network infrastructure using a non-authorized portable media device and without detection. Without controls in place to detect, deter, or prevent this type of activity, malicious insiders could remove sensitive information with the intent to compromise the security and mission of DNDO.

- Sensitive Email Content Testing: We conducted testing to determine if emails with sensitive and PII markings and caveats, as defined in *DHS Management Directive 11042.1* and *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, could be sent outside of DNDO without being detected. Without controls in place to deter or prevent this type of activity, malicious insiders could exfiltrate sensitive unclassified information through DNDO's electronic mail service with the intent to compromise the security and mission of DNDO.

- Wireless Security Checks for Unauthorized Devices: We performed visual inspections and conducted security testing using tools that run wireless scans. The testing assessed whether wireless security is controlled and monitored to prevent unauthorized systems and devices from connecting to DNDO/DHS networks. Without controls in place to deter or prevent this type of activity, a malicious insider could use unauthorized wireless activities to compromise the security and mission of DNDO.

We conducted this performance audit between June 2013 and November 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate DNDO's efforts to provide the necessary information and access to accomplish this audit. Appendix C contains major OIG contributors to this report.

Appendix B
Management Comments to the Draft Report

Domestic Nuclear Detection Office
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 22, 2014

MEMORANDUM FOR: The Honorable John Roth
Inspector General
Office of Inspector General

FROM: Huban A. Gowadia, Ph.D.
Director

SUBJECT: OIG Draft Report: "Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, but Challenges Remain" (Project No. 13-148-ITA-DNDO)

Thank you for the opportunity to review and comment on this draft report. The Domestic Nuclear Detection Office (DNDO) appreciates the U.S. Department of Homeland Security (DHS), Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

We are pleased to note OIG's recognition that DNDO has taken steps to address and mitigate the insider risk at DNDO, including participation in the Under Secretary of Intelligence and Analysis' Insider Threat Task Force. DHS's Office of Chief Security Officer (OCSO) is also providing security awareness training to DNDO employees and contractors that is designed to mitigate and detect insider risk, among other on-going activities.

We agree the draft findings and recommendations in this report can be used as a basis to strengthen the effectiveness and efficiency of DHS and DNDO information technology (IT) and insider threat programs. Specifically, the OIG recommended that the Director of DNDO:

Recommendation 1: Implement insider threat procedures, upon receipt of policy issued by DHS OCIO, that defines roles and responsibilities for addressing insider risks to unclassified networks and systems.

Response: Concur. DNDO OCIO and DHS OCIO agree that insider threat policies and procedures that define roles and responsibilities, from network to user level, are fundamental for addressing insider risks to unclassified networks and systems. Accordingly, DHS OCIO has developed related policy documented in DHS Sensitive Systems Policy Directive 4300A, that meets all of the requirements recommended by the United States Computer Emergency Readiness Team (US-CERT), except for protection

For Official Use Only

of intellectual property. The relevant policy statements can be found in the following sections of this directive:

- Acceptable use of IT resources: Section 4.1.2, "Rules of Behavior" and Section 4.8.5, "Personal Use of Government Office Equipment and DHS Systems/Computers"
- Monitoring of IT resources: Section 4.1.2, "Rules of Behavior," Section 4.8.5, "Personal Use of Government Office Equipment and DHS Systems/Computers," and Section 5.2.3, "Warning Banner"
- Managing employee use of social media: Section 3.16, "Social Media"
- Employee resignations and separations: Section 4.1.6, "Separation from Duty"

DNDO will document its implementation of the existing policy by December 31, 2014. No later than December 31, 2014, DHS OCIO will: (1) develop and incorporate policy in Directive 4300A addressing the protection of intellectual property and (2) work with DNDO OCIO to identify any additional insider threat-related requirements beyond Directive 4300A with which DNDO needs to comply. DNDO OCIO will then expeditiously document its implementation of the revised Directive 4300A and the additional requirements, if any.

Estimated Completion Date (ECD): December 31, 2014.

Recommendation 2: Provide documentation that clearly shows the effectiveness of controls or processes in place to detect and respond to unauthorized data exfiltration from DNDO unclassified IT assets via email services provided by OCIO.

Response: Concur. DNDO will coordinate with DHS OCIO to ensure the latter implements the required security controls or processes, and provides DNDO documentation of their effectiveness. DHS OCIO already has a data loss prevention solution at the gateway that monitors emails for extrusion, which is monitored for anomalous traffic, that, when identified, results in actions being taken, as appropriate. A mandated requirement to detect and respond to unauthorized data exfiltration via email applications on unclassified networks, however, has not yet been codified in either federal or agency policy, consequently, funding for implementing a technical means to satisfy such a requirement and the full intent of this recommendation does not exist at this time.

DNDO OCIO has discussed and coordinated with DHS OCIO about this matter, which is beyond DNDO's authority to address on its own. DHS OCIO advised that once guidance and funding is in place, they will provide additional architecture solutions and implementation, as appropriate. Given the actions taken to address this recommendation and the fact that additional actions are beyond DNDO's authority, DNDO requests that OIG consider this recommendation resolved and closed.

Recommendation 3: Disable portable media ports on unclassified IT devices under direct DNDO control where no business need exists to have them enabled.

Response: Concur. DNDO OCIO agrees that the use of portable media devices can pose a potential threat, and, as such, will implement appropriate controls and processes on portable media ports for systems owned and registered by DNDO. For systems where ports remain active in order to satisfy business requirement, documentation will be provided explaining implementation and operation of risk mitigating process controls. ECD: December 31, 2014.

Recommendation 4: Apply critical security patches on DNDO IT assets in accordance with DHS security policy.

Response: Concur. DHS OCIO and DNDO OCIO recognize that DHS information might be subject to unauthorized access and disclosure through exploit of vulnerabilities potentially discoverable in select DHS information technology assets. DHS OCIO and DNDO OCIO aggressively and regularly apply security patches to their information systems, per the Information System Vulnerability Management (ISVM) process. DHS OCIO ensures that all DHS OCIO information technology assets, which include assets used by DNDO, have the latest software security upgrades as directed by US-CERT or requests waivers or exceptions for ISVM's necessary for legacy systems that cannot be upgraded within the time listed for compliance by US-CERT. Accordingly, DNDO requests that OIG consider this recommendation resolved and closed.

Recommendation 5: Perform periodic security assessments of DNDO sites to identify unauthorized wireless devices or connections

Response: Concur. DNDO OCIO and DHS OCIO agree that periodic wireless assessments of DHS HQ sites, which include those used by DNDO, to identify unauthorized connections to DHS information technology assets, such as an external network, is a helpful tool in managing insider threat risk. Accordingly, DHS OCIO has already taken steps to implement technology and processes that will enable such assessments. Specifically, the LAN A Information Systems Security Officer conducts periodic wireless assessments of DHS HQ locations within the National Capital Region on a regular basis for unauthorized wireless connections. Further, DNDO and DHS OCIO will formalize the periodicity of the assessments conducted at DNDO. Any connection suspected of an insider threat risk is evaluated to determine if it is connected to a DHS IT asset, and if so, it is disconnected and reported per DHS policy, as appropriate. Accordingly, DNDO requests that OIG consider this recommendation resolved and closed.

Again, thank you for the opportunity to review and comment on this draft report. Technical Comments were previously provided under separate cover. However, given that the draft recommendations have been revised since the initial draft, we have submitted additional Technical Comments to address potential inconsistencies between the revised recommendations and the text of the draft report, and to address sensitivity issues. We look forward to working with you in the future.

Appendix C
Major Contributors to This Report

Richard Saunders, Director
Philip Greene, Audit Manager
Scott He, Lead IT Specialist
Jason Dominguez, IT Specialist
Michael Horton III, Management and Program Assistant
Greg Wilson, Management and Program Assistant
Kelly Herberger, Communications Analyst
Anna Hamlin, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Director of Local Affairs, Office of Intergovernmental Affairs
Chief Privacy Officer
Chief Information Officer
Chief Information Security Officer

Domestic Nuclear Detection Office

DNDO Director
DNDO Chief of Staff
DNDO Chief Information Officer
DNDO Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.