



Why This Matters

To improve the Nation's capability to detect nuclear or radiological material for use against the United States, the Domestic Nuclear Detection Office (DNDO) employee's access its operations, systems, and data. Based on job function or role, these trusted insiders are typically given access to mission-critical assets.

Trusted insiders could use their access or insider knowledge to exploit DNDO's physical and technical vulnerabilities with the intent to cause harm. Types of insider threats could include spying, release of information, sabotage, corruption, impersonation, theft, smuggling, and terrorist attacks.

DHS Response

Our report had five recommendations, if implemented, should strengthen DNDO's security posture against the risk posed by trusted insiders.

DNDO concurred with all of the recommendations.

For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

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

What We Determined

Steps are underway to address and mitigate the insider risk at DNDO. 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, including DNDO. The DHS Office of Intelligence and Analysis has detailed a counterintelligence officer to DNDO to help mitigate espionage-related insider risks and routinely briefs DNDO on counterintelligence awareness, including insider threat indicators. DNDO provides security awareness training to its employees and contractors that includes security-related topics that could help prevent or detect the insider risk. In 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 that may have been caused by insiders.

Additional steps can be taken to address the insider risk at DNDO by implementing insider threat procedures, documenting the effectiveness of controls or process in place to detect and respond to unauthorized data exfiltration from DNDO, disabling portable media ports where no business needs exists, applying critical information technology (IT) security patches, and performing security assessments to identify unauthorized wireless devices or connections.

What We Recommend

We recommended that the Director for DNDO:

- 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.
- 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.
- 3) Disable portable media ports on unclassified IT devices under direct DNDO control where no business need exists to have them enabled.
- 4) Apply critical security patches on DNDO IT assets in accordance with DHS security policy.
- 5) Perform periodic security assessments of DNDO sites to identify unauthorized wireless devices or connections.