



## DITMAC Frequently Asked Questions (FAQ)

### What is the DITMAC?

DITMAC is the Department of Defense (DoD) Insider Threat Management and Analysis Center. DITMAC is the DoD's enterprise insider threat hub. DITMAC collaborates with DoD leaders and the 43 DoD Components to oversee mitigation, prepare risk assessments and recommendations, and synchronize responses to potential and actual insider threats.

### Why was the DITMAC established?

DITMAC was established to implement the March 18, 2014 report, *Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews*. This report summarized the internal and independent review directed by the Secretary of Defense to identify ways the DoD can improve its security programs, policies, and procedures following the shooting attack by Aaron Alexis on September 16, 2013. Alexis killed 12 people and injured 3 others inside the Washington Navy Yard.

The Alexis shootings reminded us that we cannot wait to defend ourselves from insiders intending to do us harm. The pattern of recent insider threats points to a broadening danger. Like Alexis, Army Major Nidal Hasan used his trusted access to DoD people and facilities to fatally shoot 13 people and injure 30 others at Ft. Hood, Texas. In addition, DoD continues to deal with damage done by Army Private Bradley Manning's unauthorized disclosures, which led to Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (enacted by the President on October 7, 2011).

Manning, like NSA contractor Edward Snowden, represents the danger of one insider threat to DoD classified information. Alexis, like Hasan, represents the danger of one insider threat to DoD personnel and facilities. DITMAC was established as the enterprise hub for DoD insider threat information management to improve our defenses against insider threat behaviors like these.

### What is an insider threat hub?

A hub is an analysis and data aggregation capability that brings people, tools, and information together to build comprehensive assessments of behaviors indicative of a potential insider threat.

Presidential Memorandum *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (signed November 21, 2012) established policy guidance for all Executive Agencies, including the DoD and its 43 Components. This memo directed the agencies to establish a centralized insider threat capability, or *hub*, as the foundation of a viable and effective insider threat program. The hub gives each agency an enterprise capability to evaluate its own risk and fulfill the requirements of the National Insider Threat Minimum Standards.



## **What is an insider threat?**

For DoD, an insider is defined as any person with authorized access to DoD resources. A person can become an insider by virtue of employment, volunteer activities, or contractual relationship with DoD. The insider threat is the breach of trust that occurs when an insider uses his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

## **Who runs the DITMAC?**

On December 12, 2014, the Under Secretary of Defense for Intelligence gave the Defense Security Service (DSS) the responsibility to incubate the DITMAC. Since then, DSS has hired the DITMAC team, funded and established its initial concept of operations, and initiated the legal and technical processes required to authorize its system of record for aggregating and analyzing insider threat information.

## **Is DITMAC operational today?**

Yes, but while in its incubation period, DITMAC will only function as a limited operation. DITMAC does not expect to be a full operational capability (FOC) until FY18. It was provisionally approved for initial operating capability (IOC) in October 2015. This allows DITMAC to receive reports from DoD Components based on an initial list of reporting thresholds (10 thresholds as of this date).

DITMAC is making significant progress. All Components were given a datasheet for reporting, which they can submit to DITMAC via SIPR email. DITMAC cannot accept or process personally identifiable information (PII) or personal health information (PHI) until its system of record notice (SORN) is approved. For properly submitted reports, DITMAC is conducting basic analysis, collaborating with Components, sending them relevant media reports, and providing basic metrics to DoD leadership.

As an organization, DITMAC has established its Concept of Operations (CONOPS), staffing plan, Standard Operating Procedures (SOPs), risk models, initial reporting thresholds, a Liaison Officer (LNO) Program, and Strategic Communications Plan.

## **What makes DITMAC unique?**

DITMAC is a unique enterprise capability. While many aspects of the insider threat mission have been the responsibility of personnel in security, human resources, counterintelligence, legal, cybersecurity, and law enforcement operations, DITMAC provides a centralized hub for bringing those areas of expertise together to aggregate and analyze information in order to support DoD and its Components. DITMAC focuses on continually improving DoD's ability to detect and respond to behaviors indicative of a potential insider threat—as incidents occur and over time.



## **Does DITMAC own the DoD insider threat mission?**

No. Each Component must manage its own insider threat program—proactively. DITMAC does not supersede, but supports, each Component’s responsibility to meet the Minimum Standards. DITMAC will not direct Components to take action on its people; it will oversee the mitigation of insider threats for DoD by identifying challenges and making recommendations to Components. DITMAC will not set insider threat policy; it will ensure policy is being implemented and will advocate for Components to DoD leadership on specific concerns, promising policy ideas, and common initiatives.

## **What agencies does the DITMAC support?**

DoD as a whole, and each of the 43 DoD Components, are required to implement the Minimum Standards. DITMAC is DoD’s enterprise hub and supports each of the Component hubs. Among the DoD Components are the Military Departments (Army, Navy, Air Force, Marines, National Guard and Joint Staff), the Defense Agencies (Defense Advanced Research Project Agency (DARPA), Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), Missile Defense Agency (MDA), and others), DoD Field Activities (Defense Technical Information Center (DTIC), Defense Health Agency (DHA), Washington Headquarters Services (WHS), and others), and Combatant Commands (AFRICOM, EUCOM, TRANSCOM, and others).

## **Do DoD insider threat programs threaten our privacy and civil rights?**

No. DITMAC, like all executive branch insider threat programs, are focused on detecting and responding to anomalous behavior, not stereotyping individuals. Insider threat programs were developed from their inception to protect privacy and civil liberties. The National Insider Threat Task Force (NITTF), co-chaired by the U.S. Attorney General and the Director of National Intelligence (DNI), developed the national insider threat program with supporting policy, standards, guidance, and training that prevent violations of privacy and civil rights.

When a person is granted authorized access to DoD resources, they sign authorizations that accept additional oversight of their workplace behaviors. DoD insider threat programs, like all insider threat programs, are designed to operate in coordination with each agency’s legal counsel, civil liberties and privacy officials, and records management office, each of which are responsible to build in protections against infringement of an employee’s civil rights, privacy, or whistleblower protections. Department and agency heads are required to ensure these protections are maintained without compromise.

## **What harm can be done without strong insider threat programs across DoD?**

The gravity of the insider threat is the fact that one person can do such grave harm. As DNI James R. Clapper stated succinctly at the NITTF Legal Forum on October 28, 2015, “One person can compromise information that can cripple our government. One person can expose the strategies that keep America



safe. One person can walk into a workplace with a weapon and commit an atrocity. The insider threat is insidious. It's hiding among the people we trust most."

The threat is not new, but the harm one insider can do in our connected age amplifies today's threat. America's national security interests depend upon proactive insider threat programs. These programs can and must be implemented without harming the civil liberties and privacy of DoD employees.

### **What is DITMAC focused on doing for the remainder of its incubation period?**

As DITMAC moves forward, targeting FY18 to achieve FOC, it will be focused on implementing its CONOPS, engaging the 43 DoD Component, building its analytic methodologies, refining its SOPs, enhancing its reporting thresholds, collaborating with LNOs, establishing effective communications, and sharing relevant insights to the insider threat community. Each of these efforts is well underway.

Two strategic priorities for the coming years will be the standing up the DITMAC System of Systems (DSoS) and resolving legal questions surrounding the DITMAC System of Records Notice (SORN). DITMAC's communications plan features regular outreach activities to keep the insider threat community informed on our progress and to elicit substantive input from key stakeholders across the community on the DSoS implementation strategy and the SORN.

### **What is the status of the DITMAC System of Systems (DSoS)?**

DSoS is DITMAC's enterprise information technology capability that supports our analysts with aggregated data and advanced processing tools. DSoS is early in its development. The DSoS Roadmap defines key elements of DSoS' core capabilities, data integration and hosting architecture, reporting workflows for Component submissions, advanced analytics, and reporting.

DSoS will not be a push-button solution that aggregates all the data and identifies insider threats with total certainty. In alignment to DITMAC's multi-disciplinary approach, DSoS will be able to aggregate multiple data sources—from counterintelligence, mental health, security, human resources, cyber, and others—to support incisive analysis and actionable recommendations by DITMAC analysts. DSoS will be, fundamentally, a support to human processes of analysis, decision making, and action.

### **What is the status of the DSoS System of Records Notice (SORN)?**

There are important legal questions to be answered before we can offer a more detailed status. Approval of a System of Records Notice (SORN) will enable DITMAC to accept and process PII/PHI. DITMAC and its legal team began drafting the SORN in 2014. The intent has been, from the beginning, to enable DITMAC to implement the DSoS and to provide a legal construct that other DoD programs can use as a more advanced starting point for their own SORN. DoD Insider Threat Policy (DoDD 5205.15) allows Components to tailor approach, so DITMAC designed its SORN to be extensible to DoD Components, if they so choose adopt the DSoS as its hub technology.