



Homeland
Security

DEC - 7 2016

ACTION

MEMORANDUM FOR THE SECRETARY

THROUGH: Francis X. Taylor *Francis X. Taylor*
Under Secretary for Intelligence and Analysis

Chip Fulghum *Chip Fulghum*
Deputy Under Secretary for Management

FROM: Richard D. McComb *Richard D. McComb*
Chief Security Officer

SUBJECT: **Expanding the Scope of the DHS Insider Threat Program**

Purpose: Approve expanding the scope of the DHS Insider Threat Program beyond the protection of classified information to include threats posed by all DHS employees.

Background or Context: Executive Order (EO) No. 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs require the head of each department or agency that operates or accesses classified computer networks to implement an insider threat detection and prevention program to safeguard classified national security information.¹

¹ The National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs that implements Executive Order No. 13587 define the terms "Insider Threat" and "Insider" as follows:

Insider Threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat 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.

Insider: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

While these definitions, read in isolation of EO 13587, appear to provide an expansive definition of the terms "Insider" and "Insider Threat," the reforms mandated by EO 13587 are limited to protecting classified information from unauthorized disclosure, and thus so are these terms.

The reforms mandated by EO 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs are limited to protecting classified information from unauthorized disclosure. Accordingly, the purpose of the DHS Insider Threat Program established pursuant to EO 13857 is scoped to prevent the unauthorized disclosure of classified national security information.²

Within the Department, the Under Secretary for Intelligence and Analysis is delegated the responsibility for overseeing the implementation of the Insider Threat Program. The Chief Security Officer serves as the DHS Senior Insider Threat Official responsible for the day-to-day management and oversight of the Insider Threat Program, subject to the guidance and direction of the Under Secretary for Intelligence and Analysis.

The Department has made great strides and implemented a robust Insider Threat Program, focused on the mandate to protect classified information, which will be at full operational capability by the end of this calendar year, consistent with the deadline set by the National Security Council in May 2014.

As we grow and mature the DHS Insider Threat Program, it has become clear that the threats the Department faces extend beyond threats to our classified information by our cleared employees. The threats we face from trusted insiders include threats posed by insiders with and without security clearances engaging in activities that have no nexus to the unauthorized disclosure of classified information. The February 12, 2012 workplace shooting at the ICE office in Long Beach, California; the February 27, 2015 arrest and subsequent conviction of a MGMT/OCIO contractor for wire fraud and conspiracy to hack into government databases; and the June 9, 2016 arrest of an I&A employee for illegally carrying a concealed weapon on to the Nebraska Avenue Complex are just three examples of the broader threats the Department faces from trusted insiders.

Neither EO 13587 nor the separately promulgated National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs authorize the Department to implement an Insider Threat Program beyond the limited mandate to protect classified information from unauthorized disclosure. While EO 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs establish government-wide baseline requirements for safeguarding classified information, they do not prohibit executive departments and agencies from expanding their Insider Threat Programs beyond the minimum requirements to safeguard classified information from unauthorized disclosure. The Office of the General Counsel

² DHS Instruction 262-05-002, "Information Sharing and Safeguard Program: Insider Threat Program," § I (July 9, 2015) ("The DHS Insider Threat Program is intended to prevent unauthorized disclosure of classified national security information, deter cleared employees from becoming insider threats, detect employees who pose a risk to classified national security information, and mitigate risks to the security of classified national security information through administrative, investigative, or other responses, while protecting the privacy and civil rights and civil liberties of DHS personnel.").

has concluded that the Department can rely upon other existing legal authorities in order to expand the Insider Threat Program within DHS beyond the scope of EO 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

As contemplated, the expanded scope of the DHS Insider Threat Program would include the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. Insiders would include any person who has or who had authorized access to any DHS facilities, information, equipment, networks, or systems.

Administering an expanded DHS Insider Threat Program beyond the protection of classified information currently extends beyond the authorities delegated to the Under Secretary for Intelligence and Analysis. However, the Under Secretary for Management possesses the necessary authorities to execute the expanded mission of the DHS Insider Threat Program. Accordingly, the Under Secretary for Intelligence and Analysis and Under Secretary for Management could jointly oversee the Department's implementation of the expanded Insider Threat Program, on your behalf, within existing legal authorities. Under this construct, the Chief Security Officer would remain responsible for day-to-day execution of the program, subject to guidance and direction from the Under Secretary for Intelligence and Analysis and Under Secretary for Management.

In accordance with your approval expanding the scope of the DHS Insider Threat Program, DHS Instruction 262-05-002, "Information Sharing and Safeguard Program: Insider Threat Program" (July 9, 2015) will be revised and reissued consistent with this memorandum.

Clearance:

PLCY: DCOS Briana Petyo, cleared w/out comments on 10/20/2016

MGMT: ACOS Laurie Boulden, cleared w/out comments on 10/18/2016

OGC: Steve McCleary, cleared w/out comments on 10/21/2016

FYI copies were circulated to Components: USCG, FEMA, ICE, USCIS, CBP, TSA, USSS.

Recommendations: Approve expanding the scope of the DHS Insider Threat Program beyond the protection of classified information to include the threats posed to the Department by all individuals with access to the Department's facilities, information, equipment, networks, or systems; and have the Under Secretary for Intelligence and Analysis and Under Secretary for Management jointly oversee the Department's implementation of the broader Insider Threat Program on your behalf under existing legal authorities.

Approve/date  1/3/17 Disapprove/date _____

Modify/date _____ Needs discussion/date _____