



SECRETARY OF THE ARMY
WASHINGTON

31 JUL 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2013-18 (Army Insider Threat Program)

1. References:

- a. Presidential Memorandum (National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs), 21 Nov 12.
- b. Army Regulation 381-12 (Threat Awareness and Reporting Program), 4 Oct 10.

2. This directive establishes the Army Insider Threat Program in accordance with reference 1a.

3. The Army Insider Threat Program is an integrated departmental effort to deter, detect and mitigate risk by employees or servicemembers who may represent a threat to national security. A comprehensive insider threat program is essential to the safety and security of our Soldiers, Families, Civilians, contractors, infrastructure and information. The Army's program will strengthen the protection of personnel, information and resources.

4. Reference 1a defines an insider threat as 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."

5. The Army will:

- a. ensure the security and safety of Army computer networks by establishing an integrated capability to monitor and audit user activity across all domains to detect and mitigate activity indicative of insider threat behavior;
- b. facilitate the sharing of counterintelligence (CI), security, information assurance (IA), law enforcement (LE), human resources (HR), and other related information to recognize and counter the presence of an insider threat;
- c. evaluate personnel security information;
- d. provide the workforce with training on insider threat awareness and their reporting responsibilities; and

SUBJECT: Army Directive 2013-18 (Army Insider Threat Program)

e. gather information to establish a centralized analysis, reporting and response capability.

6. Responsibilities

a. The Assistant Secretary of the Army (Manpower and Reserve Affairs) and Deputy Chief of Staff (DCS), G-3/5/7 are designated as the Army Senior Officials responsible for providing management, accountability and oversight and for recommending resources for the Army Insider Threat Program. They will:

(1) provide general oversight for the Army Insider Threat Program;

(2) make sure all insider threat program activities, including training, are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies; and

(3) ensure the close coordination of efforts across the Army Secretariat and Staff.

b. The DCS, G-1 will facilitate the sharing of applicable HR information with authorized personnel, consistent with law and policy, that will allow them to recognize the presence of an insider threat.

c. The DCS, G-2 will:

(1) facilitate the sharing of CI, security and other related information with the IA, LE and HR components of the Army Insider Threat Program to recognize the potential for or actual presence of an insider threat;

(2) evaluate and use all required personnel security information;

(3) establish and maintain a Threat Awareness and Reporting Training Program that incorporates behavioral indicators of concern and mandated CI and security reporting responsibilities;

(4) establish and maintain a security education and reporting program;

(5) develop and oversee implementation of a technical capability to monitor user activity on the Joint World Intelligence Communication System and coordinate with the Army Chief Information Officer (CIO)/G-6 on the development and oversight of a similar capability to be employed on other Army classified information systems; and

(6) support an integrated, centralized analysis, reporting and response capability to detect and mitigate threats.

SUBJECT: Army Directive 2013-18 (Army Insider Threat Program)

d. The DCS, G-3/5/7 will:

- (1) be the proponent for the policy in this directive;
- (2) establish and maintain an integrated, centralized analysis, reporting and response capability for the detection and mitigation of insider threats; and
- (3) ensure that the provisions of this directive are incorporated into appropriate Army regulations, the Army Planning and Programming Guidance, and the Army Programming Guidance Memorandum as soon as practicable.

e. The Army CIO/G-6 will:

- (1) develop and oversee, in coordination with the Department of Defense (DoD) CIO, implementation of a technical capability to monitor user activity on the Secure Internet Protocol Router Network and any other Army classified computer network for which the Army (CIO/G-6) is responsible for conducting network operations;
- (2) ensure, in coordination with the DoD CIO and Office of the Army General Counsel, that cleared Army employees sign user agreements acknowledging that their activity on any Army classified or unclassified computer network, including portable electronic devices, is subject to monitoring and could be used against them in a criminal, security or administrative proceeding;
- (3) ensure, in coordination with the DoD CIO and Office of the Army General Counsel, that banners for the Army's classified and unclassified computer networks are established informing users that their network activity is being monitored for lawful U.S. Government purposes and can result in criminal or administrative actions against the user;
- (4) coordinate with the DCS, G-2 to facilitate the sharing and synchronizing of user activity monitoring and data auditing across all computer networks to detect activity indicative of insider threat behavior; and
- (5) provide the Army Insider Threat Program all relevant classified and unclassified IA data from all computer networks.

f. The Provost Marshal General will:

- (1) facilitate the sharing of applicable criminal intelligence and LE information consistent with privacy laws, civil liberties and regulations to authorized personnel in the CI, IA and HR components of the Army Insider Threat Program to recognize the potential for or actual presence of an insider threat;

SUBJECT: Army Directive 2013-18 (Army Insider Threat Program)

(2) oversee an integrated, centralized analysis, reporting and response capability for the detection and mitigation of insider threats;

(3) establish an LE-based awareness and reporting program; and

(4) develop a capability to vet personnel for access to Army facilities against authoritative U.S. Government databases to identify potential criminals, terrorists or other security and insider threats.

g. The Army General Counsel will review the Army Insider Threat Program for legality and consistency with reference 1a.

h. The Judge Advocate General will review the Army Insider Threat Program for legality and consistency with reference 1a.

i. The Surgeon General will provide information from medical sources, consistent with privacy laws and regulations, to authorized personnel to help them recognize the presence of an insider threat.

j. All Headquarters, Department of the Army Principal Officials, commanders, Army organizations and personnel shall support the DCS, G-3/5/7 in executing this directive and implementing the Army Insider Threat Program as it evolves.

k. The Army Civil Liberties Officer will ensure that any civil rights and civil liberties issues are appropriately addressed as future insider threat efforts are implemented across the Army.

l. Army Protection Program

(1) The Army Protection Program Board of Directors will provide the senior-level oversight to ensure cross-functional coordination among Headquarters, Department of the Army Principal Officials and commanders.

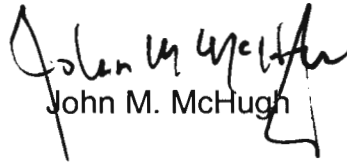
(2) The Army Protection Program management framework (Council of Colonels, General Officer Steering Committee and Board of Directors) will track and monitor development of the Army Insider Threat Program.

(3) As the Army Insider Threat Program matures, the Office of the DCS, G-3/5/7 (G-34) will conduct self-assessments of compliance with policies and standards during scheduled Army Protection Program assessments.

7. Administrative publications affected by this directive will be identified, reviewed and revised to incorporate this guidance within 6 months of the date of this directive.

SUBJECT: Army Directive 2013-18 (Army Insider Threat Program)

8. This directive is effective immediately.



John M. McHugh

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army
Commander

- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade

CF:

Director, Army National Guard
Director of Business Transformation