(U) Results in Brief

(U) Followup Audit on the Military Departments' Security Safeguards Over SIPRNET Access Points

(U) March 18, 2019

(U) Objective

(U) We determined whether the actions Army, Navy, and Air Force officials took to correct the problems identified in prior DoD Office of Inspector General reports improved logical and physical security safeguards that protect SECRET Internet Protocol Router Network (SIPRNET) access points. Specifically, we reviewed the security safeguards protecting SIPRNET access points at Fort Huachuca, Arizona; Fort Hood, Texas; Naval Station Norfolk, Virginia; Naval Air Station North Island, California; Joint Base Langley-Eustis, Virginia; and Offutt Air Force Base, Nebraska.

(U) Background

~~(FOUO)~~ [redacted]

(U) SIPRNET access points are logical or physical connections where users can access the network. Logical safeguards are system-based mechanisms, such as firewalls, permission settings, and SIPRNET tokens, used to designate who or what has access to a specific system or function. Physical safeguards include locks, guards, and security containers to deter or delay access to the network.

(U) Access to the SIPRNET requires a SECRET-level clearance and a need to know the classified information transmitted on the network. The SIPRNET is an obvious target for cyber attacks and other adverse actions because it contains high-value information. Therefore, the DoD requires that Components employ logical and physical security safeguards to protect access to the SIPRNET.

(U) Findings

(U) Army, Navy, and Air Force officials did not correct problems identified in prior DoD Office of Inspector General reports related to the improvement of logical or physical security safeguards that protect SIPRNET access points. Specifically, among other findings, Army, Navy, and Air Force officials did not:

- ~~(S)~~ [redacted]
- (U) ensure that approving officials maintained completed and approved user access forms because officials did not have a process to verify the accuracy and completeness of SIPRNET access forms;
- (U) ensure users had the required security training because officials did not have a process to verify users completed the required annual security training; or
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

(U) Results in Brief

(U) Followup Audit on the Military Departments' Security Safeguards Over SIPRNET Access Points

(U) Findings (cont'd)

(U) Because the SIPRNET supports classified war-fighting and planning applications, the problems we identified with the Army, Navy, and Air Force logical or physical security safeguards could pose a risk to the life and safety of DoD personnel, impact Military programs and operations, and lead to accidental or negligent exposure of classified information on the SIPRNET.

(U) Recommendations

(U) Among other recommendations, we recommend that the Army, Navy, and Air Force Chief Information Officers:

- ~~(S)~~ [redacted]
- (U) ensure that SIPRNET access request forms are properly completed, reviewed, and approved;
- (U) ensure that SIPRNET users complete all required security training; and
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

(U) Management Comments and Our Response

(U) The Principle Deputy DoD Chief Information Officer, responding for the DoD Chief Information Officer, provided oral comments on the draft report indicating that the DoD Chief Information Officer is still working to address the recommendations related to logical and physical security safeguards; therefore, the recommendations are unresolved. We request that the DoD Chief Information Officer provide comments on the final report.

(U) In addition, based on management comments, we redirected recommendations related to physical security safeguards over the Army SIPRNET to the Army Deputy Chief of Staff for Intelligence and the Army Provost Marshal General. Therefore, we also request that they provide comments on the final report.

(U) The Acting Deputy Director for Cybersecurity, Office of the Army Chief Information Officer, responding for the Army Chief Information Officer, agreed with the recommendations to implement processes related to logical security safeguards stating that the Army Chief Information Officer will review policy gaps and issue new policy within 1 year after the final report is issued. Therefore, those recommendations are resolved and will be closed once we verify that the new policies fully address the recommendations.

(U) Results in Brief

(U) Followup Audit on the Military Departments' Security Safeguards Over SIPRNET Access Points

(U) Comments (cont'd)

~~(FOUO)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

(U) Please see the Recommendations Table on the next page.