U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Issue Date: 01/13/2016
Reissue Date (Revision 01): 11/28/2017

Policy Directive 034-03

MEMORANDUM FOR: Distribution List

FROM: Russell C. Deyo
Under Secretary for Management

SUBJECT: Continuous Improvement of Department of Homeland Security Cyber Defenses

Since the Cyber Sprint of the summer of 2015, DHS has made significant progress in enhancing its cybersecurity. However, the threats we face are advanced and persistent, and it is essential that DHS continually improve our cyber defenses.

Within 45 days of the signature of this Policy Directive, Components will take the following steps to protect their networks and educate their employees.

1. *Establish the ability to complete searches for indicators of compromise within 24 hours.*
2. *Harden and protect computers by following principles of least privilege.* Ensure no users have local administrative rights and privileges on their network-connected workstations.
3. *Achieve 100 percent two-factor authentication for users on Homeland Secure Data Network (HSDN) through the use of the HSDN Tokens.*

Within 60 days of the signature of this Policy Directive, Components will take the following steps to protect their networks.

1. *Implement technology to thwart phishing attacks.* Components deploy to Initial Operational Capability (IOC), solutions to prevent the activation of malicious links or attachments in phishing emails.
2. *Redouble our education efforts.* DHS requires that all personnel complete Information Technology Security Awareness Training on an annual basis. All of the training provided includes a section on phishing and its prevention. All personnel will complete this training, as directed by Component leadership, consistent with the timelines in this Policy Directive. Employees and contractors who have not completed the training within the required timeframe will have their network accounts disabled. Component Chief Information Security Officers are allowed to grant a one-week extension.

3. *Arm employees against social engineering.* Establish Component social engineering awareness programs to raise employee awareness about the threat of social engineering. Ensure programs conduct semi-annual tests, to include spear-phishing exercises, which cover all privileged users, all users of high value assets, and a representative sample of the remainder of the population.

Within 90 days of signature, Components will take the following step to protect their networks.

1. *Implement technology to thwart phishing attacks.* Components deploy to Full Operational Capability (FOC), solutions to prevent the activation of malicious links or attachments in phishing emails.

If a Component is unable to comply with any of the above steps by the mandated deadlines, they will submit an Elevated Risk Acceptance memorandum through the Component Head to the Under Secretary for Management by the relevant mandated deadline. The Elevated Risk Acceptance memorandum will include corrective plans of actions and milestones for meeting the requirements.

Updates of the Elevated Risk Acceptance memorandum are due quarterly following the date of submission, until compliance is completed. Quarterly updates include updates of progress against the existing Elevated Risk Acceptance memorandum, based upon the "Strengthening DHS Cyber Defenses" order dated July 22, 2015.

I and my staff, including the Office of the Chief Information Officer, stand ready to support your teams in achieving these important objectives. Address any questions to Jeff Eisensmith, DHS Chief Information Security Officer, at 202.233.3070 or Jeffrey.Eisensmith@hq.dhs.gov.

Thank you very much for your assistance and collaboration as we work to strengthen the DHS cyber infrastructure.

Distribution:

Under Secretary for Management
Under Secretary for National Protection and Programs Directorate
Under Secretary for Science and Technology
Under Secretary for Office of Intelligence and Analysis
Commandant, U.S. Coast Guard
Commissioner, U.S. Customs and Border Protection
Administrator, Federal Emergency Management Agency
Administrator, Transportation Security Administration
Assistant Secretary, U.S. Immigration and Customs Enforcement
Assistant Secretary, Office of Legislative Affairs
Assistant Secretary, Office of Policy
Assistant Secretary, Office of Public Affairs
Director, U.S. Citizenship and Immigration Services
Director, Domestic Nuclear Detection Office
Director, Federal Law Enforcement Training Center
Ombudsman, Citizenship and Immigration Services
Chief Privacy Officer
Civil Rights and Civil Liberties Officer
General Counsel
Inspector General
Director, Operations Coordination
Director, U.S. Secret Service
Assistant Secretary, Office of Health Affairs/Chief Medical Officer
Chief Financial Officer
Chief Human Capital Officer
Chief Information Officer
Chief Procurement Officer
Chief Readiness Support Officer
Chief Security Officer
Chief Information Officer, U.S. Citizenship and Immigration Services
Chief Information Officer, U.S. Coast Guard
Chief Information Officer, Transportation Security Administration
Assistant Commissioner & Chief Information Officer, U.S. Customs & Border Protection
Chief Information Officer, Domestic Nuclear Detection Office
Chief Information Officer, Federal Emergency Management Agency
Chief Information Officer, Federal Law Enforcement Training Centers
Chief Information Officer, Intelligence and Analysis
Chief Information Officer, U.S. Immigration and Customs Enforcement
Chief Information Officer, National Protection and Programs Directorate
Chief Information Officer, Office of Health Affairs
Chief Information Officer, Science and Technology
Chief Information Officer, U.S. Secret Service