Posted on: May 09, 2007

(U) EXECMessage-164: "Information Systems Security Awareness"

Distribution: Senior Executive Message to the Workforce

POC: Kevin P. Ford [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) As you heard recently from the Director, we each have responsibilities "to ensure the security of our information and the continued availability of our information technology assets."

[redacted] (b)(3)-P.L. 86-36

As you know, our SIGINT, Information Assurance (IA), and the Joint Functional Component Command for Network Warfare (JFCC-NW) missions can be successful only when our Information Technology Infrastructure (ITI) is available and secure. Just as NSA is interested in collecting foreign intelligence, NSA resources are targets for foreign intelligence collection. We must guard against all threats, to include insiders, in order to make sure our IT is robust and ready to support our nations' security needs.

(U//~~FOUO~~) [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) Some things we all must do to ensure security and availability:

- (U) Be vigilant.

- (U//~~FOUO~~) Prevent the introduction of malicious code: do not download unauthorized data from the internet or other electronic media. Protect our ITI from malicious code including worms, viruses, and Trojans that could damage or destroy our SIGINT and IA capabilities.

- (U//~~FOUO~~) Limit the use of bandwidth on the unclassified system for non-mission activities. This could result in the unintended

(b)(3)-P.L. 86-36

consequence of denying service to our mission elements.

- (U//~~FOUO~~) Lock your screen when leaving the area. Do not let others masquerade as you or access data for which they are not cleared (protect the ITI from an insider threat).

- (U//~~FOUO~~) Do not divulge classified information on the Internet.

- (U//~~FOUO~~) Notify the Security Health Officer (SHO) if you are aware of unusual happenings on the system, 963-5636:

[redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) Remember, U R critical to secURity! The following documents are always available for your reference:

- NSA/CSS Policy 6-3, NSA/CSS Operational Information Systems Security Policy

[redacted] (b)(3)-P.L. 86-36

and NSA/CSS Manual 130-1, Operational Information Systems Security Manual

[redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) Stay tuned for information about the updated refresher course in the near future. If you have any questions, please contact your ISSPM:

[redacted] (b)(3)-P.L. 86-36

Kevin Ford
Director for Information Technology, Chief Information Officer

UNCLASSIFIED//FOR OFFICIAL USE ONLY