DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

APR 24 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Data Call to Confirm Compliance on Measures for Safeguarding and Handling of Classified National Security Information

Reference: Secretary of Defense Memorandum, "Immediate Review and Assessment of Department of Defense Information Security Procedures," April 17, 2023

As noted in the referenced Secretary of Defense's April 17, 2023 memorandum, Services/Components have until May 2, 2023 to review and assess their adherence to cybersecurity and other standards relating to the protection of classified national security information. Additionally, each DoD Service/Component shall review their implementation of the actions below and report their compliance with the cybersecurity controls specified in Committee on National Security Systems Instruction (CNSSI) 1253 as laid out in the attachment and within the CNSS Directive 504 regarding deployment and implementation of User Activity Monitoring (UAM) on National Security Systems. These include access control, auditing, and UAM across the Secret Internet Protocol Router Network and TOP SECRET systems (e.g., Joint Worldwide Intelligence Communications System (JWICS)) that process, store, and transmit classified information.

Specifically, by May 26, 2023, Services/Components via their Chief Information Officers (CIOs) must certify their compliance of the systems and networks the Component owns and/or manages to DoD CIO via the CyberScope tool on the following activities outlined below and, in the attachment, which DoD CIO will incorporate into its cybersecurity scorecard:

1. **Implementation of Least Privilege and Access Control security controls**.

   a. System owners of data repositories must take measures to restrict access to classified data (to including limitations on printing of classified information, review of distribution lists, and requirements to encrypt emails) based on need to know in addition to all other requirements for access to such classified information and not simply level of clearance.

   b. System owners review and minimize the privileges for software products to execute (e.g., review/minimize the privileges associated with system service accounts).

   c. System owners review and remove privileged accounts and access for any individual who no longer requires such access.

2. **Ensure optimized audit capabilities**. System owners must ensure auditing capabilities are activated on systems processing, storing, or transmitting classified information, including SharePoint sites and other collaboration capabilities and that the events captured meet baseline required events for classified systems as outlined in CNSSI 1015.

3. **Optimized UAM capabilities.** System owners must deploy UAM capabilities, triggers, and analysis on classified endpoints, along with:

    a. Ensuring that UAM capabilities are actively managed and monitored by insider threat cells or similar organizations.

    b. Validating the status of their UAM programs on systems providing web hosting and collaboration capabilities for TOP SECRET data (i.e., Intelink, etc.) on TOP SECRET systems (e.g., JWICS).

The DoD CIO will work with the Intelligence Community CIO in the Office of the Director of National Intelligence (ODNI) and the Under Secretary of Defense for Intelligence and Security to guide implementation of the above actions on systems hosting Sensitive Compartmented Information (SCI) data. Reporting of SCI systems, including JWICS, will be through ODNI channels. The DoD CIO will also finalize minimum UAM triggers and, when published, DoD Services/Components will ensure that insider threat cells or similar units leverage these triggers as part of their comprehensive insider threat program. My point of contact for this effort is [redacted]

John B. Sherman

Attachment:
As stated

Attachment

Least Privilege and Access Control

- **Least Privilege**
  - AC-6 Least Privilege
  - AC-6(1) LP – Authorize Access to Security Functions
  - AC-6(2) LP – Non-privileged Access for non-security functions
  - AC-6(5) LP – Privileged Accounts
  - AC-6(7) LP – Review of User Privileges
  - AC-6(8) LP – Privilege Levels for Code Execution
  - AC-6(9) LP – Auditing use of Privileged Functions
  - AC-6(10) LP – Prohibit Non-Privileged Users from Executing Privileged Functions
- **Access Control**
  - AC-1 Access Control Policy and Procedures
  - AC-2 Account Management
  - AC-2(7) Account Management – Role Based Schemes
  - AC-3 Access Enforcement

Audit Logging and Monitoring

- **Audit Logging**
  - AU-1 Audit and Accountability Policy and Procedures
  - AU-2 Audit events
  - AU-2(3) Audit Events – Reviews and Updates
  - AU-9 Protection of Audit Information
  - AU-10 Non-Repudiation
- Determine whether component guidance on the auditable events incorporates the events mandated in CNSSI 1015 Annex B

User Activity Monitoring

- Validate implementation and compliance with:
  - DoD Directive 5205.16 Sec. 3 Sub C
  - DoD Instruction 8530.01 Sec. 3 Sub C (6)
  - 100% implementation of UAM capabilities on classified endpoints
    - % UAM deployed on SIPR
    - % UAM deployed on JWICS
    - % endpoints having UAM actively monitored for SIPR and JWICS
    - Longer-term, % endpoints being monitored for min triggers