Results in Brief

Audit of Contingency Planning for DoD Information Systems

August 21, 2019

Objective

The objective of this audit was to determine whether DoD Components consistently developed and tested information system contingency plans (ISCP), as required by DoD and Federal guidance, for the recovery of national security systems (NSS) and data after emergencies, system failures, or disasters.

We selected a nonstatistical sample of 15 NSSs to review from six DoD Components. Specifically, we reviewed six Army, four Navy, two Air Force, one Marine Corps, one Missile Defense Agency, and one Washington Headquarters Services.

We conducted initial site visits from September 2016 to March 2017 to understand the systems and the environment they operate in and to obtain any relevant contingency planning documentation. We conducted followup site visits from July to October 2018 to request the current ISCPs and testing documentation to ensure that we reported on relevant and accurate ISCP documentation.

Background

A national security system is an information system that involves intelligence activities, cryptologic activities related to national security, command and control of military forces, weapon or weapons system equipment, or the direct fulfillment of military or intelligence missions. Disruption of an information system could result in the inability to complete mission operations.

Background (cont'd)

DoD guidance requires DoD Component heads to develop ISCPs and conduct testing to recover information system services following an emergency or other disruption. DoD guidance also states that all DoD information systems must identify its impact level and apply the appropriate security controls based on the corresponding impact level.

Findings

DoD Components did not consistently develop and test ISCPs to recover NSSs and data after emergencies, system failures, or disasters as required by DoD and Federal guidance. Specifically, we found that the system owners:

- developed and tested ISCPs for 2 of the 15 systems in accordance with minimum ISCP requirements;
- developed ISCPs for 9 of the 15 systems, but the ISCPs did not contain all minimum ISCP requirements or test the ISCPs; and
- did not develop or test ISCPs for 4 of the 15 systems.

This occurred because the DoD Chief Information Officer (CIO), the DoD Component heads, and their CIOs did not prioritize and ensure that ISCPs were consistently developed and tested for NSSs, as required.

~~(FOUO)~~ Without a valid ISCP, DoD Components may not effectively recover NSSs or data in a timely manner or minimize the negative impact to critical missions after emergencies, system failures, or disasters, [redacted]

Recommendations

~~(FOUO)~~ We recommend that the DoD CIO update DoD guidance to require that DoD Component heads develop and test an ISCP in accordance with DoD guidance and verify and conduct periodic reviews to ensure that all NSSs have a developed and tested ISCP. We also recommend that those responsible

Recommendations (cont'd)

~~(FOUO)~~ for contingency planning in the Army, Navy, Air Force, Missile Defense Agency, and Washington Headquarters Services [redacted] in accordance with DoD guidance.

Management Comments and Our Response

The DoD CIO disagreed with the recommendations to update DoD guidance to require that DoD Component heads develop and test ISCPs and conduct periodic reviews to ensure ISCPs are developed and tested for all NSS but proposed alternative actions to emphasize the importance of contingency planning. However, the DoD CIO endorsed a memorandum issued by the DoD Senior Information Security Officer to reiterate the requirements for DoD Components' to implement contingency planning requirements in the context of their mission, operational environment, and organizational conditions. We believe that the memorandum itself does provide sufficient guidance to DoD and addresses the recommendation we made in this report. Therefore, the recommendations to update DoD guidance for contingency planning are closed and no further comments are required.

The Army CIO, responding for of the Secretary of the Army, agreed to issue implementation guidance. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive documentation showing that the actions have been implemented.

~~(FOUO)~~ The Office of the CIO Director for the Under Secretary of the Navy, responding for the Secretary of the Navy, agreed to [redacted] The Director also stated that the Marine Corps agreed

~~(FOUO)~~ with the overall recommendation for the DoD CIO to clarify guidance regarding the type of systems requiring an approved plan, such as [redacted] However, the Director did not state what actions the Marine Corps would take to [redacted]. Therefore, the recommendation is unresolved and the Director should provide additional comments describing how the Marine Corps will [redacted]

~~(FOUO)~~ The Air Force Chief Information Security Officer, responding for the Secretary of the Air Force, did not agree or disagree with the recommendation. The Chief Information Security Officer stated that the Air Force requires program managers to [redacted] and that DoD and Federal guidance does not require [redacted]. However, DoD guidance requires that system owners [redacted] Therefore, the recommendation is unresolved and the Chief Information Security Officer should provide additional comments describing what actions the Air Force will take to [redacted].

~~(FOUO)~~ The Missile Defense Agency Director agreed with the recommendation but did not describe the actions the Missile Defense Agency plans to take to [redacted] The Missile Defense Agency Director stated that the agency [redacted]

Comments (cont'd)

~~(FOUO)~~ [redacted] Therefore, the recommendation is unresolved and the Director should provide additional comments describing how the Missile Defense Agency will [redacted]

~~(FOUO)~~ The Washington Headquarters Services, Financial Management Directorate Acting Director, responding for the Washington Headquarters Services Director, disagreed with the recommendations; [redacted] This action would meet the intent of the recommendation by [redacted]

~~(FOUO)~~ [redacted] Therefore, that recommendation is resolved but will remain open. We will close the recommendation once we receive documentation [redacted]. However, the recommendation to [redacted] in accordance with DoD guidance is unresolved. We request that the Acting Director provide additional comments describing how WHS will [redacted].

Please see the Recommendation Table on the next page for a status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
DoD Chief Information Officer			1.a, 1.b
Secretary of the Army		2	
Secretary of the Navy	3		
Secretary of the Air Force	4		
Director, Missile Defense Agency	5		
Director, Washington Headquarters Services	6.b	6.a	

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.