Results in Brief

(U) Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions

March 13, 2020

(U) Objective

(U) The objective of this followup audit was to determine whether DoD Cyber Red Teams and DoD Components took actions to correct problems identified in Report No. DODIG-2013-035, "Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness," December 21, 2012. In addition, we determined whether DoD Cyber Red Teams supported operational testing and combatant command exercises to identify network vulnerabilities, threats, and other security weaknesses affecting DoD systems, networks, and facilities, and whether corrective actions were taken to address DoD Cyber Red Team findings. We also assessed risks affecting the ability of DoD Cyber Red Teams to support DoD missions and priorities.

(U) Background

(U) DoD Cyber Red Teams are independent, multi-disciplinary groups of DoD personnel that are certified, accredited, and authorized to identify vulnerabilities that impact the confidentiality, integrity, or availability of DoD systems and networks by portraying the tactics, techniques, and procedures of adversaries. The DoD uses DoD Cyber Red Teams to highlight vulnerabilities, improve joint cyberspace operations, and protect the DoD Information Network and DoD weapons systems from vulnerabilities and threats that affect the DoD's security posture. Unlike traditional vulnerabilities, such as misconfigured security settings and unpatched software, DoD Cyber Red Teams use known vulnerabilities, zero day attacks (attacks that exploit a previously unknown hardware, firmware, or software vulnerability), and other tactics an adversary may use to penetrate systems, networks, and facilities, and test the defense-in-depth strength (use of multiple barriers and layers of defenses

(U) Background (cont'd)

(U) to protect systems, networks, and organizations and responses taken to DoD Cyber Red Team actions. As of September 2019, the National Security Agency accredited 10 DoD Cyber Red Teams.

(U) Summary of Prior Report

~~(U//FOUO)~~ In our prior report, issued in December 2012, we determined that DoD Cyber Red Teams did not effectively report the results of their assessments to the assessed organizations; the Director, Operational Test and Evaluation; U.S. Cyber Command; the Joint Force Headquarters-DoD Information Network; and other DoD Cyber Red Teams. In addition, we found that the DoD Components did not effectively correct or mitigate [redacted] Red Team-identified vulnerabilities and did not track or report the vulnerabilities on a plan of action and milestones as required by the Chairman of the Joint Chiefs of Staff Instruction 6510.01F. Furthermore, we found that the DoD Cyber Red Team certification and accreditation process did not effectively assess the skills of the DoD Cyber Red Teams and their ability to perform mission functions and meet training requirements.

~~(U//FOUO)~~ In that report, we recommended that U.S. Strategic Command [redacted]. In addition, we recommended that the Services develop procedures to:

- ~~(U//FOUO)~~ [redacted]
- ~~(U//FOUO)~~ [redacted]
- ~~(U//FOUO)~~ [redacted]

Results in Brief

(U) Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions

(U) Summary (cont'd)

- ~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ We also recommended that the assessed organizations [redacted]. Lastly, we recommended that U.S. Strategic Command and the National Security Agency [redacted] to perform their mission functions as part of the certification and accreditation process. The DoD Components agreed with all of the prior report's recommendations and agreed to take corrective actions.

(U) Findings

~~(U//FOUO)~~ For this followup audit, we determined that the DoD Components did not consistently mitigate or include unmitigated vulnerabilities identified in the prior audit and during this audit by DoD Cyber Red Teams during combatant command exercises, operational testing assessments, and agency-specific assessments in plans of action and milestones. Specifically, of the [redacted] DoD Cyber Red Team-identified vulnerabilities that we assessed, DoD Components:

- ~~(U//FOUO)~~ mitigated [redacted] vulnerabilities,
- ~~(U//FOUO)~~ did not mitigate [redacted] vulnerabilities, and
- ~~(U//FOUO)~~ partially mitigated [redacted] vulnerabilities.

(U) The DoD Components did not consistently mitigate vulnerabilities or include unmitigated vulnerabilities in plans of action and milestones because they failed to assess the impact of the vulnerabilities to their mission, prioritize resources to implement risk mitigation solutions, or coordinate the results of DoD Cyber Red Team reports with applicable stakeholders addition,

(U) the DoD did not have an organization responsible for ensuring that DoD Components took action to manage vulnerabilities identified by DoD Cyber Red Teams and did not establish processes that held DoD Components responsible for mitigating those vulnerabilities.

~~(U//FOUO)~~ [redacted] Ensuring DoD Components mitigate vulnerabilities is not only essential to achieve a better return on investment [redacted] and continues to invest on DoD Cyber Red Team activities [redacted].

(U) In addition, we determined that the DoD did not establish a unified approach to support and prioritize DoD Cyber Red Team missions. Instead, the DoD Components implemented Component-specific approaches to staff, train, and develop tools for DoD Cyber Red Teams, and prioritize DoD Cyber Red Team missions. The DoD did not establish a unified approach because the DoD did not:

- (U) assign an organization with responsibility to oversee and synchronize DoD Cyber Red Team activities based on DoD needs and priorities;

Results in Brief

(U) Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions

(U) Findings (cont'd)

- (U) assess the resources needed for each DoD Cyber Red Team and identify core requirements to staff and train them to meet DoD priorities; or
- (U) develop baseline tools to perform assessments.

(U) Without an enterprise-wide solution to staff, train, and develop tools for DoD Cyber Red Teams and prioritize their missions, DoD Cyber Red Teams have not met current mission requests and will not meet future requests because of the increased demands for DoD Cyber Red Team services. Until the DoD assigns an organization to assess DoD Cyber Red Team resources, it will be unable to determine the number of DoD Cyber Red Teams and staffing of each team to support mission needs, which will impact the DoD's ability to identify vulnerabilities and take corrective actions that limit malicious actors from compromising DoD operations.

(U) Recommendations

(U) We recommend that the Secretary of Defense assign an organization with responsibility to, among other actions:

- (U) review and assess DoD Cyber Red Team reports for systemic vulnerabilities and coordinate the development and implementation of enterprise solutions to mitigate those vulnerabilities;
- (U) ensure DoD Components develop and implement a risk-based process to assess the impact of DoD Cyber Red Team-identified vulnerabilities and prioritize funding for corrective actions for high-risk vulnerabilities;
- (U) ensure DoD Components develop and implement processes for providing reports with DoD Cyber Red Team findings and recommendations to organizations with responsibility for corrective actions;
- (U) develop processes and procedures to oversee DoD Cyber Red Team activities, including synchronizing and prioritizing DoD Cyber Red Team missions, to ensure these activities align with DoD priorities;
- (U) perform a joint DoD-wide mission-impact analysis to determine the number of DoD Cyber Red Teams, minimum staffing levels of each team, the composition of the staffing levels needed to meet current and future DoD Cyber Red Team mission requests;
- (U) assess and identify a baseline of core and specialized training standards, based on the three DoD Cyber Red Team roles that DoD Cyber Red Team staff must meet for the team to be certified and accredited; and
- (U) identify and develop baseline tools needed by DoD Cyber Red Teams to perform missions.

(U) We recommend that the Chairman of the Joint Chiefs of Staff revise Chairman of the Joint Chiefs of Staff Instruction 6510.05 and Chairman of the Joint Chiefs of Staff Manual 6510.02 to include requirements for addressing DoD Cyber Red Team-identified vulnerabilities and reporting actions taken to mitigate those vulnerabilities.

(U) Furthermore, we recommend that the Commanders for U.S. Strategic Command and U.S. Southern Command, Program Manager Advance Amphibious Assault for the Amphibious Combat Vehicle; and Director for the Defense Forensics and Biometric Agency assess and prioritize the risk of each unmitigated vulnerability identified in the Red Team assessments, take immediate actions to mitigate high-risk vulnerabilities, and if unable to immediately mitigate the vulnerabilities, include them on a command-approved plan of action and milestones.

Results in Brief

(U) Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions

(U) Management Comments and Our Response

(U) This report contains 14 recommendations addressed to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, Commanders for U.S. Southern Command and U.S. Strategic Command, Program Manager Advanced Amphibious Assault for the Amphibious Combat Vehicle, and the Director for the Defense Forensics and Biometric Agency. Of the 14 recommendations, 13 are resolved but will remain open until further actions are taken, and 1 was closed. Below is a description of management comments to the 14 recommendations.

(U) The Deputy to the Principal Cyber Advisor, responding for the Secretary of Defense, agreed with all recommendations. The Deputy stated that the DoD would leverage the results of assessments required by Sections 1660 and 1652 of the National Defense Authorization Act for FY 2020 to review the roles, responsibilities, and processes for adjudicating, disseminating, and monitoring DoD Cyber Red Team activities and improve follow up and implementation actions to mitigate DoD Cyber Red Team findings affecting weapon systems, warfighting platforms, and defense critical infrastructure.[1]

(U) The Director for Joint Staff, responding for the Chairman of the Joint Chiefs of Staff, agreed to revise Chairman of the Joint Chiefs of Staff Instruction 6510.05 and Chairman of the Joint Chiefs of Staff Manual 6510.02 to include requirements for addressing DoD Cyber Red Team identified vulnerabilities and reporting actions taken to mitigate those vulnerabilities.

(U) The U.S. Southern Command's Director for the Communication Systems Directorate, responding for the Commander for U.S. Southern Command, agreed with the recommendation and provided configuration screenshots, policies, and procedures to support mitigation efforts for 19 of the 41vulnerabilities identified in this report.

(U) The Director for Command, Control, Communications, and Computers Systems, responding for the Commander for U.S. Strategic Command, agreed with the recommendation to mitigate vulnerabilities identified in this report.

(U) The Deputy Program Manager Advanced Amphibious Assault for the Amphibious Combat Vehicle 1.1, responding for the Program Manager Advanced Amphibious Assault, agreed to develop a plan of action and milestones for unmitigated vulnerabilities by February 29, 2020.

(U) The Deputy Provost Marshall General for the Army, responding for the Director for the Defense Forensic and Biometric Agency, neither agreed nor disagreed with the recommendation, but provided documentation that supported wireless scanning occurred regularly. Therefore, the recommendation is closed.

(U) Please see the Recommendations Table on the next page for the status of recommendations.

[1] (U) Public Law 116–92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019. Section 1660, "Joint Assessment of Department of Defense Cyber Red Team Capabilities, Capacity, Demand, and Requirements," and Section 1652, "Zero-Based Review of Department of Defense Cyber and Information Technology Personnel, "December 20, 2019.

(U) Recommendations Table

(UNCLASSIFIED) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Secretary of Defense		A.5.a, A.5.b, A.5.c, A.5.d, A.5.e, B.1.a, B.1.b, B.1.c, B.1.d	
Chairman of the Joint Chiefs of Staff		A.6	
Commander for U.S. Southern Command		A.1	
Commander for U.S. Strategic Command		A.2	
Program Manager Advanced Amphibious Assault for the Amphibious Combat Vehicle		A.3	
Director for the Defense Forensics and Biometric Agency			A.4 **(UNCLASSIFIED)**

(U) 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 action were implemented.