

~~SECRET//NOFORN~~

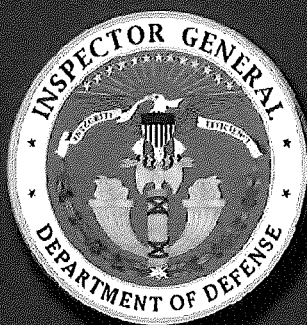
Report No. DODIG-2013-035

December 21, 2012

# Inspector General

United States

Department of Defense



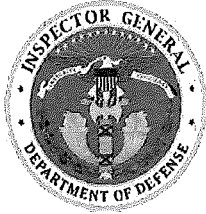
Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness (U)

Classified By: DoDIG (b)(6)  
Derived from:  
Declassify on: ~~January 7, 2037~~

Copy 33 of 33

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



Department of Defense  
Office of Inspector General

---

(U) **Better Reporting and Certification  
Processes Can Improve Red  
Teams' Effectiveness**

**Project No. D2011-D000LC-0242.000**

December 21, 2012

*We are issuing this proposed report to obtain comments and a statement of actions management will take. We may revise this report as a result of comments received and further reviews by the Department of Defense Office of Inspector General.*

~~*Distributing this proposed report outside DoD is not authorized. You must safeguard this report to prevent publication or improper disclosure of the information in the report.*~~

Classified By: DoDIG (b)(6), Readiness, Operations,  
and Support  
Derived From: Multiple Sources  
Declassify On: ~~20370107~~

~~SECRET//NOFORN~~

**(U) Additional Copies**

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or contact the Secondary Reports Distribution Unit at [auditnet@dodig.mil](mailto:auditnet@dodig.mil).

**(U) Suggestions for Audits**

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing at [auditnet@dodig.mil](mailto:auditnet@dodig.mil), or by mail:

Department of Defense Office of Inspector General  
Office of the Deputy Inspector General for Auditing  
ATTN: Audit Suggestions/13F25-04  
4800 Mark Center Drive  
Alexandria, VA 22350-1500

DEPARTMENT OF DEFENSE

**hotline**

**To report fraud, waste, mismanagement, and abuse of authority.**

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900  
Phone: 800.424.9098 e-mail: [hotline@dodig.mil](mailto:hotline@dodig.mil) [www.dodig.mil/hotline](http://www.dodig.mil/hotline)

**(U) Acronyms and Abbreviations**

1 <sup>st</sup> IO	1 <sup>st</sup> Information Operations
ABIS	Automated Biometric Identification System
AFI	Air Force Instruction
AR	Army Regulation
ATG	Adversary Tactics Group
BIMA	Biometrics Identity Management Agency
BIOS	Basic Input Output System
C&A	Certification and Accreditation
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	Computer Network Defense
COCOM	Combatant Command
ENTSG	USS Enterprise Strike Group
FISMA	Federal Information Security Management Act of 2002
GHWSBG	USS George H.W. Bush Strike Group
IAS	Information Aggressor Squadron
IDS	Intrusion Detection System
JFHQ	Joint Forces Headquarters
NIPRNET	Non-secret Internet Protocol Router Network
NSA	National Security Agency
OMB	Office of Management and Budget
PEO-EIS	Program Executive Office, Enterprise Information Systems
POA&M	Plan of Action and Milestones
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedures
USFLTFORCOM	U.S. Fleet Forces Command
USSTRATCOM	U.S. Strategic Command



~~SECRET//NOFORN~~  
INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
4800 MARK CENTER DRIVE  
ALEXANDRIA, VIRGINIA 22350-1500

December 21, 2012

(U) MEMORANDUM FOR COMMANDER, U.S. STRATEGIC COMMAND  
COMMANDER, U.S. CYBER COMMAND  
ASSISTANT SECRETARY OF THE AIR FORCE  
(FINANCIAL MANAGEMENT AND COMPTROLLER)  
DIRECTOR, NATIONAL SECURITY AGENCY/  
CHIEF, CENTRAL SECURITY SERVICE  
NAVAL INSPECTOR GENERAL  
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

(U) SUBJECT: Better Reporting and Certification Processes Can Improve  
Red Teams' Effectiveness (Report No. DODIG-2013-035)

(U) We are providing this report for your review and comment. The DoD Cyber Red Teams did not effectively report vulnerabilities, threats, and infiltration activities to assessed organizations and DoD Components. In addition, the assessed organizations did not correct or mitigate all vulnerabilities and did not report all security weaknesses. Finally, U.S. Strategic Command and the National Security Agency officials did not include reviews and analysis of Red Team members' proficiency, training, and certifications in their Certification and Accreditation process. This can lead to

DoDIG (b)(7)(E)

[REDACTED] We considered management comments on a draft of this report when preparing the final report.

(U) DoD Directive 7650.3 requires that recommendations be resolved promptly. Management Comments from the Secretary of the Army; Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army; Director, Biometrics Identity Management Agency; Program Executive Officer, Enterprise Information Systems were responsive and no further comments are required. The U.S. Fleet Forces Command and 377<sup>th</sup> Air Base Wing did not comment on a draft of this report. We request comments from the Commander, U.S. Fleet Forces Command and the Commander, 377<sup>th</sup> Air Base Wing. Management Comments from some respondents were partially responsive. We request additional comments from U.S. Strategic Command on Recommendation C.1.d. We request additional comments from the National Security Agency/Central Security Service on Recommendations B.1, B.2, C.1.b, C.1.c, and C.1.d. We request additional comments from U.S. Fleet Cyber Command/U.S. Tenth Fleet on Recommendation A.5.b. We request additional comments from the Joint Forces Headquarters Kansas on Recommendation B.1. We request additional comments from the 57<sup>th</sup> Adversary Tactics Group on Recommendations A.6.b and A.6.c. In addition, as a result of management comments, we revised Recommendations A.3, B.1, B.2, and C.1 for the National Security Agency/Central Security Service and redirected Recommendations A.4.a and A.4.b to U.S. Army Cyber Command/2<sup>nd</sup> Army.

(U) We should receive your comments by January 31, 2013. Comments provided must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01, volume II. Please provide comments that state whether you agree or disagree with the findings and recommendations. If you agree with our recommendations, describe what actions you have taken or plan to take to accomplish the recommendations and include the completion dates of your actions. If you disagree with the recommendations or any

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
4800 MARK CENTER DRIVE  
ALEXANDRIA, VIRGINIA 22350-1500

(U) part of them, please give specific reasons why you disagree and propose alternative action if that is appropriate.

(U) Please provide comments that conform to the requirement of DoD Directive 7650.3. If possible send a portable document file (.pdf) containing your comments to <sup>DoD IG (b)(6)</sup> [redacted]@dodig.smil.mil and <sup>DoD IG (b)(6)</sup> [redacted]@dodig.smil.mil. We are unable to accept the /Signed/ symbol in place of the actual signature. Classified comments must be sent electronically over the Secret Internet Protocol Router Network (SIPRNET).

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-<sup>DoD IG (b)(6)</sup> [redacted] (DSN 664-<sup>DoD IG (b)(6)</sup> [redacted]).



Alice F. Carey  
Assistant Inspector General  
Readiness, Operations, and Support

~~SECRET//NOFORN~~



## (U) Results in Brief: Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness

### (U) What We Did

(U) Our audit objective was to assess the effectiveness of DoD Cyber Red Teams' activities. Specifically, we determined whether the Red Teams followed DoD and Components' standard operating procedures (SOPs) when evaluating or testing for vulnerabilities, threats, infiltration controls, or other services performed on Components' systems. Also, we determined whether Components implemented the recommendations and tracked findings through resolution. Lastly, we determined whether U.S. Strategic Command (USSTRATCOM) and National Security Agency (NSA) certified and accredited Red Teams in accordance with DoD standards.

### (U) What We Found

(U) The Red Teams used and followed Rules of Engagement instead of SOPs when testing for vulnerabilities. However, Red Teams produced incomplete reports and did not always provide the reports to the appropriate DoD Components. This occurred because:

- the Navy and Air Force Red Team Commanders determined it was more efficient to produce generic recommendations and did not consider some findings significant enough to report.
- the Army and Air Force Red Teams agreed to not release reports outside of the assessed organizations, the Navy Red Team considered the reports part of an internal operation, and the NSA Red Team did not distribute the reports because they needed approval.

As a result, the assessed organizations may not immediately correct vulnerabilities and DoD

(U) Components cannot analyze the information to determine systemic network vulnerabilities.

(U) Also, assessed organizations did not effectively correct or mitigate 15 of 59 vulnerabilities, and all 6 assessed organizations did not appropriately track or report vulnerabilities. This occurred because the assessed organizations incorrectly assumed personnel corrected the vulnerability, policies were difficult to enforce, did not have funding available, were unaware of the findings, were unable to determine a solution, and did not view vulnerabilities as reportable. Consequently, unnecessary risk of exploitation and data leaks exists on DoD networks.

(U) In addition, USSTRATCOM and NSA Certification and Accreditation process did not test Red Teams' ability and skills to perform mission functions and training requirements. This occurred because:

- USSTRATCOM and NSA did not develop minimum qualification standards.
- NSA made a management decision not to evaluate training and certification requirements in the certification rating.

As a result, Red Teams may not be as proficient as necessary to conduct thorough and realistic tests of the DoD Components.

### (U) What We Recommend

(U) USSTRATCOM should develop a standard reporting format that incorporates policies to ensure Red Teams report all findings. The assessed organizations should establish and implement policies to correct or mitigate, track, and report all security weaknesses in compliance with Federal and DoD requirements.

(U) USSTRATCOM and NSA should develop minimum qualification standards and evaluate Red Team qualifications to perform their mission functions.

**(U) Management Comments and Our Response**

(U) As a result of management comments, we redirected two recommendations for Finding A; revised one recommendation for Finding A, two recommendations for Finding B, and one recommendation for Finding C; and renumbered eight recommendations for Finding A. The U.S. Fleet Forces Command and 377<sup>th</sup> Air Base Wing did not comment on the draft of this report. We request that the

(U) USSTRATCOM, NSA/Central Security Service, U.S. Fleet Forces Command, U.S. Fleet Cyber Command/U.S. Tenth Fleet, Joint Forces Headquarters Kansas, 57<sup>th</sup> Adversary Tactics Group, and 377<sup>th</sup> Air Base Wing provide comments in response to this report. We should receive your comments by January 31, 2013. Please see the recommendations table on the next page.

(U) Although not required, we received unsolicited management comments from the Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army regarding the recommendations for Finding A; and from the Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet regarding the recommendations for Findings A and C.

**(U) Recommendations Table**

<b>Management</b>	<b>Recommendations Requiring Comment</b>	<b>No Additional Comments Required</b>
Secretary of the Army		A.1
Commander, U.S. Strategic Command	C.1.d	A.2, C.1.a, C.1.b, C.1.c, C.1.e
Director, National Security Agency/ Chief, Central Security Service	B.1, B.2, C.1.b, C.1.c, C.1.d	A.3, C.1.a, C.1.e
Commander, U.S. Army Cyber Command/2 <sup>nd</sup> Army		A.4.a, A.4.b
Commander, U.S. Fleet Forces Command	B.3	
Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet	A.5.b	A.5.a
Adjutant General, Joint Forces Headquarters Kansas	B.1	B.4
Director, Biometrics Identity Management Agency		B.1, B.5
Program Executive Officer, Enterprise Information Systems		B.1, B.6
Commander, 57 <sup>th</sup> Adversary Tactics Group	A.6.b, A.6.c	A.6.a, A.6.d
Commander, 377 <sup>th</sup> Air Base Wing	B.1, B.7	

**(U) Please provide comments by January 31, 2013.**



## (U) Table of Contents

(U) <b>Introduction</b>	1
(U) Objective	1
(U) Background	1
(U) Review of Internal Controls	3
(U) <b>Finding A. Red Teams Need to Complete and Distribute Beneficial Reports</b>	5
(U) Red Team Rules of Engagement	6
(U) Army and National Security Agency (NSA) Red Teams Produced Complete Vulnerability Assessment Reports	7
(U) Navy and Air Force Red Teams Produced Incomplete Vulnerability Assessment Reports	7
(U) Red Teams Did Not Appropriately Distribute Vulnerability Assessment Reports	10
(U) Conclusion	11
(U) Recommendations, Management Comments, and Our Response	12
(U) Management Comments on the Internal Controls	18
(U) <b>Finding B. Assessed Organizations Need to Correct or Mitigate, Track, and Report Security Weaknesses</b>	19
(U) Correct or Mitigate, Track, and Report Vulnerabilities	19
(U) Vulnerabilities Were Not Fully Corrected or Mitigated	19
(U) Assessed Organizations Need to Track and Report Vulnerabilities	26
(U) Conclusion	28
(U) Management Comments on the Finding and Our Response	29
(U) Recommendations, Management Comments, and Our Response	29
(U) <b>Finding C. Improvements Needed for the Certification and Accreditation (C&amp;A) Process</b>	34
(U) C&A Process Did Not Include a Review of Proficiency, Training, and Certification	34
(U) Air Force Red Team Certification Vote Did Not Have a Quorum	36
(U) <sup>NSA (b)(3)</sup> [REDACTED]	37
(U) Conclusion	37
(U) Recommendations, Management Comments, and Our Response	38

**(U) Table of Contents (cont'd)**

**(U) Appendices**

(U) A. Scope and Methodology 42

(U) Red Team Missions Selected for Review 42

(U) Red Team C&A Process Review 43

(U) Use of Computer Processed Data 44

(U) Use of Technical Assistance 44

(U) Prior Coverage 44

(U) B. Supplemental Background Information 45

(U) C. Federal and DoD Guidance 47

**(U) Glossary 50**

**(U) Management Comments**

(U) Department of the Army 52

(U) U.S. Strategic Command 53

(U) National Security Agency/Central Security Service 57

(U) U.S. Army Cyber Command/2nd Army 63

(U) U.S. Fleet Cyber Command/U.S. Tenth Fleet 66

(U) Joint Forces Headquarters Kansas 69

(U) Biometrics Identity Management Agency 70

(U) Program Executive Office, Enterprise Information Systems 73

(U) 57<sup>th</sup> Adversary Tactics Group 75

**(U) Annex. Sources 76**

## (U) Introduction

### (U) Objective

(U) Our objective was to assess the effectiveness of Cyber Red Teams' (Red Teams) activities. Specifically, we determined whether the Red Teams followed DoD and Components' standard operating procedures (SOPs) when evaluating or testing for vulnerabilities, threats, infiltration controls, or other services performed on Components' systems. Also, we determined whether Components implemented the recommendations and tracked findings through resolution. During the audit, we reviewed the Certification and Accreditation (C&A) process to determine whether Red Teams used SOPs. Specifically, we determined whether DoD Cyber Red Teams were certified and accredited in accordance with DoD standards and applicable guidance. See Appendix A for the Scope and Methodology.

### (U) Background

(U) President Barack Obama identified cybersecurity as one of the most serious economic and national security challenges that we face as a nation, but one that we are not adequately prepared to counter. The Comprehensive National Cybersecurity Initiative helps to secure the United States in cyberspace. One of the major goals is to establish a front line of defense against today's threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government.

~~(S//REL USA, FVEY)~~

OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



### (U) Red Team Overview

~~(FOUO)~~ DoD Red Teams perform an important role in enhancing awareness of network vulnerabilities, threats, and events. DoD Instruction (DoDI) O-8530.2, "Support to

---

<sup>1</sup> (U) Execute Order – An order issued by the Chairman of the Joint Chiefs of Staff with the authority of the Secretary of Defense.

(FOUO) Computer Network Defense (CND),” March 9, 2001, states that Red Teams are an Information Assurance component that is “essential to gauge the state of CND operational readiness of the DoD Components and the networks that sustain their operations” on the Global Information Grid. The Global Information Grid is the interconnected network that facilitates information to warfighters, policymakers, and support personnel. The Global Information Grid supports DoD National Security and related Intelligence activities on both classified and unclassified networks for all operating locations (including bases, mobile platforms, or deployed sites). Red Teams emulate the capabilities and methods of an adversarial force against Top Secret, Secret, and unclassified information systems. The Red Teams are critical to DoD because they assess the vulnerabilities that can affect the security of the information on the Global Information Grid.

(U) We reviewed four certified and accredited Red Teams: National Security Agency (NSA), Army, Navy, and Air Force. Red Teams perform their normal missions based on requests from other organizations (military bases, DoD Components, or COCOMs). Once an organization has requested Red Team services and been accepted for a mission, the Red Team completes a Memorandum of Understanding/Rules of Engagement (Rules of Engagement), which are used for testing of vulnerabilities. The Rules of Engagement includes assessment details, such as mission dates, objectives, and scope. The Rules of Engagement also outline agreed upon control parameters, including network boundaries, halting conditions, reconnaissance objectives, exploitation objectives, mission specific requirements, and reporting.

(U) The Red Team vulnerability assessments reviewed were:

- ~~NSA (b)(3)~~
- the Biometrics Identity Management Agency (BIMA)/Automated Biometric Identification System (ABIS)<sup>2</sup>, assessed by the Army Red Team;
- the USS George H.W. Bush Strike Group (GHWBSG), assessed by the Navy Red Team;
- the USS Enterprise Strike Group (ENTSG), assessed by the Navy Red Team;
- the Joint Forces Headquarters (JFHQ) Kansas, assessed by the Air Force Red Team; and
- the 377<sup>th</sup> Air Base Wing at Kirtland Air Force Base, New Mexico, assessed by the Air Force Red Team.

(U) For an overview of the Red Teams and the COCOM exercises, see Appendix B.

### (U) **Certification and Accreditation Process**

(FOUO) DoD Directive (DoDD) O-8530.1, “Computer Network Defense (CND),” January 8, 2001; and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E,

---

<sup>2</sup> (U) Program Executive Office, Enterprise Information Systems owns ABIS, which is the network reviewed by the Army Red Team.



~~(FOUO)~~

NSA: (b)(3)

[REDACTED]

~~(FOUO)~~

NSA: (b)(3)

[REDACTED]

**(U) Review of Internal Controls**

(U) DoDI 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of controls. We identified internal control weaknesses for the USSTRATCOM; NSA; U.S. Fleet Forces Command (USFLTFORCOM); Fleet Cyber Command/U.S. Tenth Fleet; JFHQ Kansas; BIMA; Program Executive Office, Enterprise Information Systems (PEO-EIS); 57<sup>th</sup> Adversary Tactics Group (ATG); 1<sup>st</sup> Information Operations (1<sup>st</sup> IO) Command; and the 377<sup>th</sup> Air Base Wing.

(U) For accreditation, USSTRATCOM and NSA did not establish minimum qualification standards for proficiency, evaluate training and certifications, regard certification voting requirements, or consider the Air Force Red Teams as separate teams.

(U) For vulnerability management, NSA, USFLTFORCOM, JFHQ Kansas, BIMA, PEO-EIS, and 377<sup>th</sup> Air Base Wing did not correct or mitigate all vulnerabilities; incorrectly assumed personnel addressed findings; and viewed the assessments as internal operations.

(U) For vulnerability assessment reporting, NSA, Fleet Cyber Command/U.S. Tenth Fleet, the 57<sup>th</sup> ATG, and the 1<sup>st</sup> IO Command determined: it to be more efficient to produce a generic template of recommendations, some findings were not significant

~~SECRET//NOFORN~~

(U) enough to report, and a briefing to the Chief Information Officer (CIO) was sufficient instead of a report. Also, they agreed to not release reports to DoD Components without approval of the assessed organization.

(U) We will provide a copy of the report to the senior officials responsible for internal controls at USSTRATCOM, NSA, USFLTFORCOM, Fleet Cyber Command/U.S. Tenth Fleet, JFHQ Kansas, BIMA, PEO-EIS, 57<sup>th</sup> ATG, 1<sup>st</sup> IO Command, and 377<sup>th</sup> Air Base Wing.

~~SECRET//NOFORN~~

## (U) Finding A. Red Teams Need to Complete and Distribute Beneficial Reports

(U) The Red Teams used Rules of Engagement instead of SOPs to control mission parameters when testing for vulnerabilities, threats, and infiltration controls. The Army and NSA Red Teams prepared complete vulnerability assessment reports with recommendations that corresponded to findings. However, the Navy and Air Force Red Teams did not always accurately report vulnerabilities to the assessed organizations.<sup>3</sup>

~~(FOUO)~~ Specifically, for four assessments, the Navy and Air Force Red Teams produced incomplete vulnerability assessment reports:

- The Navy Red Team provided two reports to USFLTFORCOM, the Commander, Strike Force Trainer Atlantic and the Fleet Cyber Command/U.S. Tenth Fleet that did not include recommendations that corresponded with the findings. This occurred because the Red Team Commander determined that prior assessments had similar findings and it was more efficient to produce a generic template of recommendations.
- The Air Force Red Team did not include 14 of 28 findings in the 377<sup>th</sup> Air Base Wing mission report because the Red Team Commander did not consider the findings significant enough to include in the report. For example, the Red Team found that Secret Internet Protocol Router Network (SIPRNET) information was stored on the Non-secret Internet Protocol Router Network (NIPRNET), but the Red Team did not include this finding in their report.
- The Air Force Red Team did not produce a report for the JFHQ Kansas mission because the Red Team Commander stated that a briefing to the CIO was sufficient.

(U) Contributing to this issue, USSTRATCOM did not identify the required elements for reporting and did not establish a standard report format for vulnerability assessment reporting in accordance with CJCSI 6510.01F.

~~(FOUO)~~ The Army, Navy, Air Force, and NSA Red Teams did not distribute six assessment reports to the appropriate DoD Components:<sup>4</sup>

- The Army Red Team did not distribute a report for the BIMA and ABIS assessment because the Red Team agreed to not release the report to other DoD Components.

---

<sup>3</sup> (U) Assessed Organizations – NSA, BIMA, PEO-EIS, 377<sup>th</sup> Air Base Wing at Kirtland AFB, JFHQ Kansas, GHWBSG, and ENTSG. The GHWBSG and ENTSG are U.S. Navy Fleets that fall under the command of USFLTFORCOM.

<sup>4</sup> (U) DoD Components – USSTRATCOM; NSA; and Director, Operational Test and Evaluation.

- ~~(FOUO)~~ The Navy Red Team did not distribute two reports for the GHWBSG and ENTSG assessments because the Red Team considered the report internal to the Navy.<sup>5</sup>
- The Air Force Red Team did not distribute two reports: one for the 377<sup>th</sup> Air Base Wing assessment because the Red Team agreed to not release the report to other DoD Components; and one for the JFHQ Kansas assessment because the Red Team briefed the vulnerability assessment results to the CIO instead of producing a report.

- ~~(FOUO)~~ NSA (b)(3) [REDACTED]

~~(FOUO)~~ As a result, the assessed organizations may not take immediate actions to correct or mitigate vulnerabilities, increasing the risk to the network security posture. Also, the DoD Components lacked full visibility of the vulnerabilities and infiltration activities to identify systemic issues.

### **(U) Red Team Rules of Engagement**

(U) The Red Teams used Rules of Engagement to control mission parameters when testing for vulnerabilities, threats, and infiltration controls. Red Team SOPs provide a common baseline for missions but do not contain procedures on handling specific missions. Since the Red Team services are requested by an organization, each mission is different based on the needs of the organization. The Rules of Engagement provided a flexible alternative to SOPs that allowed the Red Team to document each organization's requirements. The Rules of Engagement included assessment details, such as mission dates, objectives, and scope. The Rules of Engagement also outlined agreed-upon control parameters, including network boundaries, halting conditions, reconnaissance objectives, exploitation objectives, mission specific requirements, and reporting. We reviewed the Rules of Engagement and determined that the Red Teams followed them when testing system vulnerabilities, threats, and infiltration controls. We reviewed the SOPs for each Red Team during our review of the C&A process.

(U) The CJCSI 6510.01E, and the following version, CJCSI 6510.01F, require COCOMs, the Services, and agencies' Red Teams to produce a vulnerability assessment report and to provide the vulnerability assessment report to the DoD Components. CJCSI 6510.01F also requires COCOMs, the Services, and agencies to provide vulnerability assessment reports to the Defense Information Systems Agency and the Defense Threat Reduction

---

<sup>5</sup> (U) Strike Group – A group of U.S. Navy ships typically comprised of an aircraft carrier; guided missile cruiser; two guided missile destroyers; attack submarine; and a combined ammunition, oiler, and supply ship.



(U) Agency. Since CJCSI 6510.01E was effective August 2007 and CJCSI 6510.01F was effective February 2011, we applied different criteria based on the date of the Red Team report.

(U) Table 1 provides a summary of the Red Team Reporting. The table identifies whether the Red Teams followed guidance when producing and distributing reports to the applicable DoD Components as required by CJCSI 6510.01E and CJCSI 6510.01F.

~~(FOUO)~~ Table 1. Summary of Red Team Reporting

Assessment (Red Team)	Produced a report	Report included all findings identified	Recommendations corresponded to the findings	Provided the report to DoD Components
BIMA/ABIS (Army)	Yes	Yes	Yes	No
GHWBSG (Navy)	Yes	Yes	No	No
ENTSG (Navy)	Yes	Yes	No	No
377 <sup>th</sup> Air Base Wing (Air Force)	Yes	No	Yes	No
JFHQ Kansas (Air Force)	No	No*	No*	No*

NSA (b)(3)

\*No report produced.

### (U) Army and NSA Red Teams Produced Complete Vulnerability Assessment Reports

~~(FOUO)~~ The Army and NSA Red Team produced two reports, as required by CJCSI 6510.01E and CJCSI 6510.01F, that incorporated all findings and provided recommendations that corresponded to each finding. These reports provided the assessed organizations with information ~~NSA (b)(3)~~

### (U) Navy and Air Force Red Teams Produced Incomplete Vulnerability Assessment Reports

~~(FOUO)~~ The Navy Red Team produced two reports that included recommendations that did not correspond to the findings listed in the assessment. The Air Force Red Team briefed the 377<sup>th</sup> Air Base Wing Commander with 28 findings, but only incorporated 14 of the 28 findings in the vulnerability assessment report. Also, the Air Force Red Team did not produce a report for the JFHQ Kansas assessment.

**(U) Navy Red Team Reports Need Recommendations That Correspond With Findings**

~~(S//NF)~~

OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

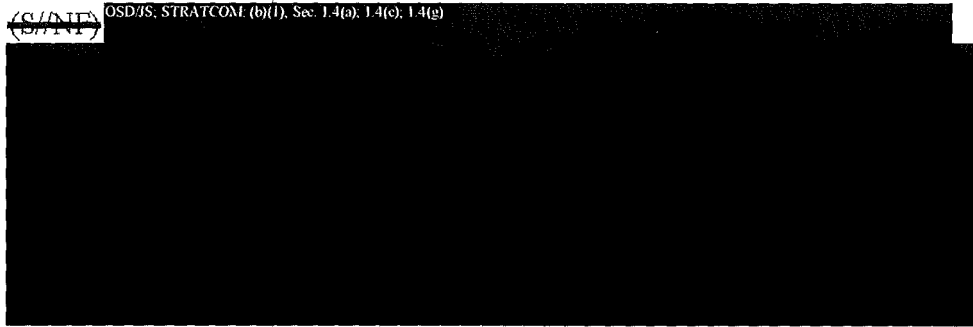


**(U) Air Force Red Team Produced an Incomplete Report**

~~(FOUO)~~ The Air Force Red Team did not include all findings in their vulnerability assessment report to the 377<sup>th</sup> Air Base Wing. The Red Team Commander did not consider 14 of 28 findings to be significant enough to report, and instead, only included them in a briefing to the 377<sup>th</sup> Air Base Wing. A Red Team report communicates a formal written account of findings, testing results, and recommendations while a briefing is an informal discussion of the findings and recommendations. Both the finalized report and a briefing are required by CJCSI 6510.01F. While there is no requirement on providing all findings in a report, the Red Team should include all findings in the finalized report to the 377<sup>th</sup> Air Base Wing. The following are examples of the significant findings not included in the report.

• ~~(S//NF)~~

OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



• ~~(S//NF)~~

OSD/JS, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



(S//NF) OSD/JS. (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



• (S//NF) OSD/JS. (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



(FOUO) The assessed organizations cannot correct or mitigate unknown vulnerabilities and cannot identify trends or systemic vulnerabilities without complete information. Red Teams should report all findings to the assessed organization to provide an assessment of the security posture.

**(U) Air Force Red Team Needs to Prepare Assessment Reports**

(FOUO) The Air Force Red Team did not produce a report for the JFHQ Kansas assessment as required by CJCSI 6510.01E. The Red Team stated they did not provide the written report because they determined that briefing the findings to the CIO was sufficient. This lack of reporting prevented the Communications Branch Chief from knowing that SIPRNET diagrams with Internet Protocol addresses stored in a shared folder on the NIPRNET was a finding. Consequently, without a report, the proper personnel cannot identify and correct or mitigate vulnerabilities and the DoD Components are unaware of the problems. The Air Force Red Team should create reports for assessed organizations.

**(U) USSTRATCOM Needs to Develop Standard Report Formats**

(FOUO) USSTRATCOM did not establish a vulnerability assessment standard report format for reporting in accordance with CJCSI 6510.01F. As a result, the vulnerability assessment reports were missing some findings and contained recommendations that did not correspond with findings, which resulted in reports that are neither beneficial nor value-added. CJCSI 6510.01F states that USSTRATCOM, as required by their Cyber Security Inspection Program responsibilities, should develop a standard report format for combatant commands, the Services, and agencies for Red Team operations. The CJCSI 6510.01F does not specifically state what elements are required in the vulnerability assessment reports; however, to add value to the report format, USSTRATCOM should identify the essential elements that should be included in all vulnerability assessment reports. Therefore, the Commander, U.S. Strategic Command, should identify required report elements and should incorporate them when developing the report format.

**(U) Red Teams Need to Provide Complete and Accurate Reports**

(FOUO) The Red Team reports should provide vital information to organizations about their network vulnerabilities and the condition or status of network defenses according to

~~(FOUO)~~ DoDI O-8530.2. When the Red Team reports are not complete or accurate and do not have findings that correlated with recommendations, it limits the assessed organization's visibility over their vulnerabilities and makes it difficult to implement the recommendations. The DoD Components receiving reports need a complete view of the network vulnerabilities and the DoD Global Information Grid security posture.

### **(U) Red Teams Did Not Appropriately Distribute Vulnerability Assessment Reports**

~~(FOUO)~~ NSA (b)(3)  
[REDACTED]

~~(FOUO)~~ NSA (b)(3)  
[REDACTED]

### **(U) Instances of Inappropriate Red Team Vulnerability Assessment Reports Distribution**

~~(FOUO)~~ The Army Red Team, their respective commands, and the assessed organization did not distribute their assessment reports to the DoD Components as required by CJCSI 6510.01E. This occurred because the Army Red Team's Rules of Engagement included agreements to not release the reports outside of the assessed organizations. The Chief of the 1<sup>st</sup> Battalion Vulnerability Assessment Detachment stated that this was to prevent outside organizations from knowing BIMA and ABIS vulnerabilities. Additionally, the Army created guidance that conflicts with CJCSI 6510.01F. Army Regulation (AR) 380-53, "Communications Security Monitoring," December 23, 2011, limits the distribution of the reports to only the assessed organization and does not distribute the reports to the DoD Components. The Army Red Team should not make agreements that contradict CJCSI 6510.01F in the Rules of Engagement, and should distribute vulnerability assessment reports to the DoD Components in accordance with CJCSI 6510.01F. The Secretary of the Army should revise AR 380-53 to not limit distribution of Red Team reports to only the assessed organizations.

~~(FOUO)~~ The Navy Red Team, their respective commands, and the assessed organization did not distribute their reports to the DoD Components as required by CJCSI 6510.01E and CJCSI 6510.01F. The Commander, Strike Force Trainer Atlantic requested the Navy Red Team to assess and report on CND of Navy Strike Groups. This Red Team assessment is a pre-deployment requirement for Navy Strike Groups. The Navy Red Team did not distribute the vulnerability assessment reports on the GHWBSG and ENTSG to the Navy Command responsible for distributing reports. This occurred



~~(FOUO)~~ because the Navy Red Team performed an internal exercise and considered the report internal to the Navy and determined the report did not need to be distributed. The Navy Red Team cannot consider reports internal just to limit distributions. The Navy has a responsibility to distribute vulnerability assessment reports to the DoD Components in accordance with CJCSI 6510.01F.

~~(FOUO)~~ Also, the Air Force Red Teams, their respective commands, and the assessed organizations did not distribute their reports to the DoD Components as required by CJCSI 6510.01F. The Air Force Red Team Commander verbally agreed not to release the report outside of the assessed organizations. Specifically, they agreed to limit the distribution to prevent outside organizations from knowing vulnerabilities at 377<sup>th</sup> Air Base Wing. The Red Teams should not make verbal agreements that contradict CJCSI 6510.01F.

~~(FOUO)~~ In addition, the Air Force Red Team did not produce a report for the JFHQ Kansas assessment as required by CJCSI 6510.01F. The Red Team stated they did not provide the written report because they determined that briefing the findings to the CIO was sufficient. Since no report was produced, the Air Force Red Team did not distribute the report to the DoD Components as required by CJCSI 6510.01F. The Air Force Red Team should create reports for assessed organizations and provide the reports to the DoD Components in accordance with CJCSI 6510.01F.

~~(FOUO)~~ The NSA Red Team and the assessed organization did not distribute their reports to the DoD Components as required by CJCSI 6510.01F. This occurred because

NSA (b)(3)



### **(U) Red Team Reports Need to Be Distributed**

~~(FOUO)~~ Without adequate report distribution as required by CJCSI 6510.01E and CJCSI 6510.01F, the organizations cannot benefit from the Red Team reports. For example, by not disseminating the information to USSTRATCOM, they are unaware of vulnerability assessment results of Red Team activities and cannot maintain a repository of the Red Team reports. This limits the network defenders' security awareness of the DoD Global Information Grid security posture. Ultimately, this may lead to unnecessary delays in correcting the vulnerabilities on DoD networks increasing the risk of loss of sensitive information, integrity, and security.

### **(U) Conclusion**

~~(FOUO)~~ The Red Teams did not always accurately report vulnerabilities and distribute the report to the assessed organizations and DoD Components. As a result, the assessed organizations may not take immediate actions to correct vulnerabilities. Also, the DoD Components do not have visibility over vulnerabilities, threats, and infiltration activities to analyze and determine systemic issues and network vulnerabilities. This ultimately limits the security awareness of the DoD Global Information Grid security posture.

~~(FOUO)~~ An adversary <sup>NSA (b)(3)</sup> [REDACTED]

## (U) **Recommendations, Management Comments, and Our Response**

### (U) ***Redirected, Renumbered, and Revised Recommendations***

(U) As a result of management comments, we renumbered draft report Recommendations A.6.a and A.6.b as A.4.a and A.4.b, respectively and redirected them from the Commander, 1<sup>st</sup> IO Command to the Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army. We renumbered Recommendations A.4.a and A.4.b as A.5.a and A.5.b, respectively. We renumbered Recommendations A.5.a, A.5.b, A.5.c, and A.5.d as A.6.a, A.6.b, A.6.c, and A.6.d, respectively. We revised Recommendation A.3 to include Chief before Central Security Service.

~~(FOUO)~~ **A.1. We recommend that the Secretary of the Army revise Army Regulation 380-53, "Communications Security Monitoring," January 23, 2011, to not limit distribution of Red Team reports to only the assessed organizations but distribute Red Team reports to the appropriate DoD components in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F.**

### (U) ***Department of the Army Comments***

(U) The Director, Counterintelligence, Human Intelligence, Disclosure and Security, responding on behalf of the Secretary of the Army, agreed with the recommendation. He stated the Office of the Deputy Chief of Staff, G-2 notified the Army Publishing Directorate of the requested change. The Director also stated the Army Publishing Directorate will publish an administrative revision to incorporate the policy change and reflect the requirements of the CJCSI 6510.01F.

### (U) ***Our Response***

(U) Comments from the Director were responsive. No further comments are required.

~~(FOUO)~~ **A.2. We recommend that the Commander, U.S. Strategic Command, develop a standard report format for Red Teams in accordance with the Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011.**

### (U) ***U.S. Strategic Command Comments***

(U) The Director, C4 Systems, responding on behalf of the Commander, USSTRATCOM, stated USSTRATCOM and U.S. Cyber Command will work with NSA Cyber Red Team to develop a standard report format. In addition, through further correspondence the Chief, Cybersecurity Assurance Division, responding on behalf of the Commander, USSTRATCOM, agreed with the recommendation.

**(U) Our Response**

(U) Comments from the Director were responsive. No further comments are required.

**(U) U.S. Army Cyber Command/2<sup>nd</sup> Army Comments**

~~(FOUO)~~ Although not required to comment, the Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army, expressed that a standard report format for Red Teams would limit their ability to employ Human Intelligence capabilities during Red Team missions.

**(U) U.S. Fleet Cyber Command/U.S. Tenth Fleet Comments**

~~(FOUO)~~ Although not required to comment, the Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet, agreed with our recommendation and stated that combined with Recommendation A.5.b, a standardized report format will allow DoD organizations to understand key information from Red Team assessments and better enable clear and consistent reporting. However, the Commander also stated that the standard format should allow each service to customize a portion due to unique configurations of assessed networks.

**(U) Our Response**

(U) The intent of a standard report format is not to limit diverse capabilities or be comprehensive, but provide the framework for capturing the required information.

~~(FOUO)~~ **A.3. We recommend that the Director, National Security Agency/Chief,**

NSA (b)(3)

[REDACTED]

**(U) National Security Agency/Central Security Service Comments**

~~(FOUO)~~ The Director, NSA/Chief, Central Security Service, NSA (b)(3)

[REDACTED]

(U) **Our Response**

(FOUO) NSA: (b)(3)

Therefore, no further comments are required.

(FOUO) **A.4. We recommend that the Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army:**

**a. Develop procedures to validate that Red Teams distribute their reports to the U.S. Strategic Command, Defense Information Systems Agency, Defense Threat Reduction Agency, and Director, Operational Test and Evaluation, in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011.**

(U) **U.S. Army Cyber Command/2<sup>nd</sup> Army Comments**

(U) The Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army, responding on behalf of the Commander, 1<sup>st</sup> IO Command, agreed with the recommendation and stated that the recommendation should have been directed to the Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army. The Commander stated the U.S. Army Cyber Command/2<sup>nd</sup> Army will implement the recommendation.

(U) **Our Response**

(U) Comments from the Commander were responsive. No further comments are required.

**b. (FOUO) Develop procedures to review agreements to determine if they contradict current DoD policies, standards, and regulations.**

(U) **U.S. Army Cyber Command/2<sup>nd</sup> Army Comments**

(U) The Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army, responding on behalf of the Commander, 1<sup>st</sup> IO Command, agreed with the recommendation and stated that the recommendation should have been directed to the Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army. The Commander stated the U.S. Army Cyber Command/2<sup>nd</sup> Army will implement the recommendation.

(U) **Our Response**

(U) Comments from the Commander were responsive. No further comments are required.

~~(FOUO)~~ **A.5. We recommend that the Commander, Fleet Cyber Command/U.S. Tenth Fleet:**

**a. Establish procedures to verify Red Team reports include recommendations that are specific to each identified finding.**

**(U) U.S. Fleet Cyber Command/U.S. Tenth Fleet Comments**

~~(FOUO)~~ The Commander, Fleet Cyber Command/U.S. Tenth Fleet, agreed and stated the Red Team final report did include some recommended mitigation, but did not address all discovered vulnerabilities. The Commander further stated the Red Team changed their final report process to ensure all identified vulnerabilities have a recommended mitigation. Also, the Commander stated the recommendations were based on an adversary's viewpoint and not a holistic or complete cyber enterprise perspective. Finally, the Commander stated the Navy Red Team is not tasked as a vulnerability mitigation organization; the Navy Red Team's primary function is to create effects during exercises and operations. Vulnerability mitigation effort needs to be coordinated throughout the cyber enterprise with the Red Team providing recommendations for mitigation.

**(U) Our Response**

(U) Comments from the Commander were responsive. No further comments are required.

**b. ~~(FOUO)~~ Develop procedures to validate that Red Teams distribute their reports to the U.S. Strategic Command, Defense Information Systems Agency, Defense Threat Reduction Agency, and Director, Operational Test and Evaluation, in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011.**

**(U) U.S. Fleet Cyber Command/U.S. Tenth Fleet Comments**

~~(FOUO)~~ The Commander, Fleet Cyber Command/U.S. Tenth Fleet, agreed with the recommendation to increase distribution of joint tasked Red Team activities through the Director, Operational Test and Evaluation as appropriate. The Commander stated that for service tasked activities, distribution should be tasked at the service level. The Red Team provides reports to the command requesting support and to Fleet Cyber Command/U.S. Tenth Fleet. Fleet Cyber Command/U.S. Tenth Fleet is the interface point for addressing identified issues.

**(U) Our Response**

(U) Although the Commander, Fleet Cyber Command/U.S. Tenth Fleet, agreed with the recommendation, the comments were not responsive. The Commander did not provide a corrective action for developing procedures that validate the Red Team reports are distributed in accordance with CJCSI 6510.01F paragraph C.6.i.(1) (b) (3), which states,

[w]hen conducting cyber security inspections or Red Team operations CC/S/As shall provide copies of final report to USSTRATCOM, DISA [Defense Information Systems Agency] (for DISN-connected IS [information systems]), NSA, DTRA [Defense Threat Reduction Agency], and DOT&E [Director, Operational Test and Evaluation].

We request that the Commander provide comments in response to the final report.

~~(FOUO)~~ **A.6. We recommend that the Commander, 57<sup>th</sup> Adversary Tactics Group:**

**a. Establish procedures to verify that Red Team reports include all findings identified.**

**(U) 57<sup>th</sup> Adversary Tactics Group Comments**

(U) The Commander, 57<sup>th</sup> ATG, neither agreed nor disagreed and stated 57<sup>th</sup> ATG personnel are modifying Information Aggressor operating standards in ATG Instruction 10-2-IAS volume 3 to include verbiage on the requirement to report mission findings in accordance with USSTRATCOM procedures. In addition, through further correspondence with the Commander, 57<sup>th</sup> IAS, he specified which comments correlated with Recommendations A.6.a, A.6.b, A.6.c, and A.6.d. (See page 75 for annotations.)

**(U) Our Response**

(U) Comments from the Commander were responsive and the corrective actions met the intent of our recommendation. Therefore, no further comments are required.

**b. ~~(FOUO)~~ Establish procedures to verify that the Red Teams create reports for all missions.**

**(U) 57<sup>th</sup> Adversary Tactics Group Comments**

(U) The Commander, 57<sup>th</sup> ATG, stated he agreed briefing operators on deviations is vital to improvement; however, the Commander stated several ways for providing assessed organizations feedback, including after action reports, technical debriefs, verbal debriefs, and lessons learned.

**(U) Our Response**

(U) Although the Commander, 57<sup>th</sup> ATG, agreed with the recommendation, the comments were not responsive regarding establishing procedures for creating reports. CJCSI 6510.01F paragraph C.6.i.(1) (a) explicitly states, “[w]hen conducting cyber security inspections or Red Team operations CC/S/As shall provide inspected or

(U) Red Team targeted organization out-briefing and coordinated final report.”  
We request that the Commander provide additional comments in response to the final report.

c. ~~(FOUO)~~ **Develop procedures to validate that Red Teams distribute their reports to the U.S. Strategic Command, Defense Information Systems Agency, Defense Threat Reduction Agency, and Director, Operational Test and Evaluation, in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, “Information Assurance and Support to Computer Network Defense,” February 9, 2011.**

**(U) 57<sup>th</sup> Adversary Tactics Group Comments**

(U) The Commander, 57<sup>th</sup> ATG, neither agreed nor disagreed and stated 57<sup>th</sup> ATG personnel are modifying Information Aggressor operating standards in ATG Instruction 10-2-IAS volume 3 to include verbiage on the requirement to report mission findings in accordance with USSTRATCOM procedures.

**(U) Our Response**

(U) Comments from the Commander were not responsive. The Commander, 57<sup>th</sup> ATG, did not address our recommendation for developing procedures that validate the Red Team reports are distributed in accordance with CJCSI 6510.01F paragraph C.6.i.(1) (b) (3), which states,

[w]hen conducting cyber security inspections or Red Team operations CC/S/As shall provide copies of final report to USSTRATCOM, DISA [Defense Information Systems Agency] (for DISN-connected IS [information systems]), NSA, DTRA [Defense Threat Reduction Agency], and DOT&E [Director, Operational Test and Evaluation].

We request that the Commander provide comments in response to the final report.

d. ~~(FOUO)~~ **Develop procedures to review agreements to determine if they contradict current DoD policies, standards, and regulations.**

**(U) 57<sup>th</sup> Adversary Tactics Group Comments**

(U) The Commander, 57<sup>th</sup> ATG, neither agreed nor disagreed and stated 57<sup>th</sup> ATG personnel are developing cross-check procedures to continually identify contradictions between Red Team SOPs and DoD guidance, which will be included in the ATG Instruction 10-2-IAS volume 3.

**(U) Our Response**

(U) Comments from the Commander were responsive and the corrective actions met the intent of our recommendation. Therefore, no further comments are required.



(U) **Management Comments on the Internal Controls**

(U) ***U.S. Army Cyber Command/2<sup>nd</sup> Army Comments***

(U) The Commander, U.S. Army Cyber Command/2<sup>nd</sup> Army, acknowledged the identified internal control issues and stated they will be remedied through implementation of Recommendations A.6.a and A.6.b, which are now Recommendations A.4.a and A.4.b respectively.

## (U) **Finding B. Assessed Organizations Need to Correct or Mitigate, Track, and Report Security Weaknesses**

(U) Assessed organizations did not fully correct or mitigate, track, or report vulnerabilities identified during Red Team assessments.<sup>6</sup> Specifically,

- 5 of 6 assessed organizations did not correct or mitigate 15 of 59 vulnerabilities identified by the Red Teams. This occurred because the assessed organizations:
  - incorrectly assumed the personnel addressed the finding,
  - policies were difficult to enforce,
  - did not have funding available,
  - were unaware of the findings, or
  - were unable to determine a solution.
- All six assessed organizations did not appropriately track or report vulnerabilities identified by the Red Teams. This occurred because the assessed organizations did not recognize Red Team findings as reportable vulnerabilities or assumed all vulnerabilities were corrected.

(U) As a result, these vulnerabilities cause unnecessary risk on DoD networks and could be exploited to gain access, obtain sensitive information, or manipulate data within the DoD Global Information Grid. Also, DoD has an incomplete knowledge of all vulnerabilities.

### (U) **Correct or Mitigate, Track, and Report Vulnerabilities**

(U) Assessed organizations are required to mitigate, track, and report information system vulnerabilities identified in accordance with DoD Directive 8500.01E, "Information Assurance (IA)," April 23, 2007, and Office of Management and Budget (OMB) guidance. Five of the six assessed organizations did not fully correct or mitigate vulnerabilities found by the Red Team, and none of the six assessed organizations appropriately tracked or reported the vulnerabilities identified.

### (U) **Vulnerabilities Were Not Fully Corrected or Mitigated**

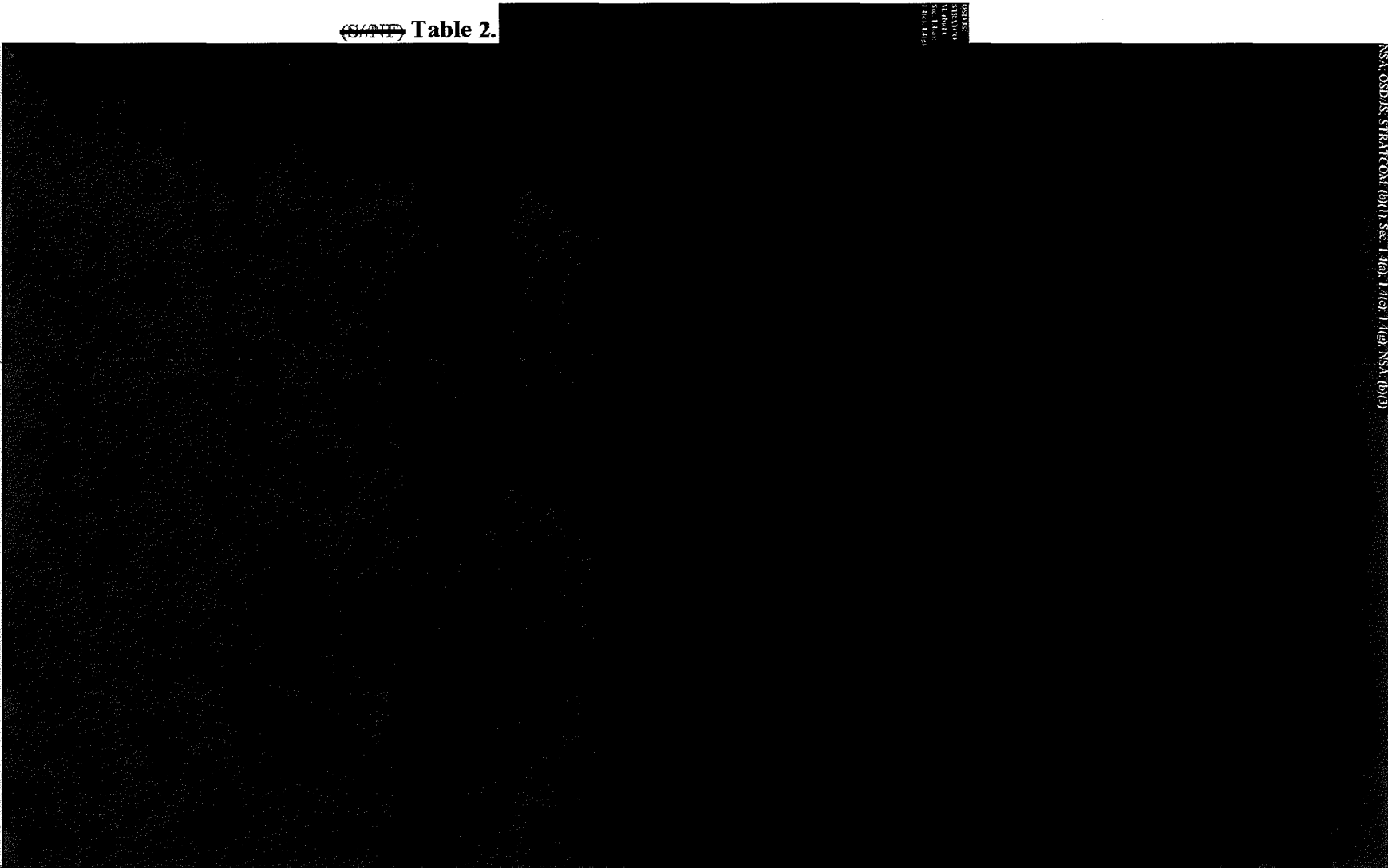
(U) DoDD 8500.01E states that organizations should mitigate and track identified information system vulnerabilities. Table 2 on page 20 summarizes the uncorrected or unmitigated vulnerabilities found by the Red Team and provides an abridgement of the details listed below. Table 2 identifies the uncorrected or unmitigated vulnerabilities, their potential impact on the organization, and the amount of time the assessed organization had to correct or mitigate the vulnerabilities.

---

<sup>6</sup> (U) Assessed Organizations – The Red Teams assessed NSA, BIMA, PEO-EIS, 377<sup>th</sup> Air Base Wing at Kirtland Air Force Base, JFHQ Kansas, GHWBSG and ENTSG for vulnerabilities. The GHWBSG and ENTSG are U.S. Navy Fleets, which fall under the command of USFLTFORCOM.

~~(S//NF)~~ Table 2.

~~SECRET//NOFORN~~



NSA, OSD/JS, STRATCOM (M), Sec. 1401, 1402, 1403, 1404, NSA (M), (S)

<sup>1</sup> (U) Tests of correcting or mitigating vulnerabilities could not be performed for the USS Enterprise, and the USS George H.W. Bush did not have any vulnerabilities identified in the GHWBSG report.

<sup>2</sup> (U) Time frame from the Report Date to the DoD OIG Site Visit.

<sup>3</sup> (U) A detrimental delay is when unauthorized users are able to access the system and manipulate, delete, steal information, or upload malicious code while network personnel determine the appropriate response to the incident.

(U) The assessed organizations did not adequately correct or mitigate 15 of 59 vulnerabilities. Table 3 provides a summary of the uncorrected or unmitigated vulnerabilities and identifies the following: the organizations assessed by the Red Teams, the Red Team responsible for the assessment, the total number of vulnerabilities identified, and the number of uncorrected or unmitigated vulnerabilities for each assessed organization.

~~(FOUO)~~ Table 3. Summary of Uncorrected or Unmitigated Vulnerabilities

Assessed Organization*	Red Team	Total Vulnerabilities	Uncorrected or Unmitigated Vulnerabilities
NSA (b)(3)			
BIMA	Army	15	3
PEO-EIS	Army	3	2
JFHQ Kansas	Air Force	10	5
377 <sup>th</sup> Air Base Wing	Air Force	28	4
<b>Total</b>			

\* ~~(FOUO)~~ Tests of correcting or mitigating vulnerabilities could not be performed for the USS Enterprise, and the USS George H. W. Bush did not have any vulnerabilities identified in the GHWBSG report.

~~(FOUO)~~

NSA (b)(3)

~~(S//NF)~~

NSA, OSD/JS, STRATCOM (b)(1), Sec. 1.4(b), 1.4(e), 1.4(g); NSA (b)(3)



<sup>7</sup> (U) For the sampling methodology, refer to Appendix A.

~~(FOUO)~~ **BIMA Did Not Sufficiently Correct or Mitigate Vulnerabilities**

~~(S//NF)~~

OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

[Redacted]

~~(S//NF)~~

OSD/JS, (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

[Redacted]

~~(S//NF)~~

OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

[Redacted]

~~(FOUO)~~ **PEO-EIS Did Not Sufficiently Correct or Mitigate Vulnerabilities**

~~(S//NF)~~

OSD/JS, (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

[Redacted]

(S//NF) OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)  
[Redacted]

(S//NF) OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)  
[Redacted]

(S//NF) OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)  
[Redacted]

~~(FOUO)~~ ***JFHQ Kansas Did Not Sufficiently Correct or Mitigate Vulnerabilities***

(S//NF) OSD/JS, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)  
[Redacted]

OSD/JS, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)  
[Redacted]

(S//NF) OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)  
[Redacted]

~~(FOUO)~~ Concerning sensitive information, JFHQ Kansas had their SIPRNET diagrams and schematics uploaded onto an unclassified network. The Red Team found this information on the shared drive, available to all users who had access to that drive. The SIPRNET diagrams included [Redacted]

During our site

~~(FOUO)~~ visit, JFHQ Kansas did not correct this vulnerability. JFHQ Kansas should remove the SIPRNET diagrams and schematics from the shared drive on the unclassified network.

~~(S//NF)~~

OSD/JS, STRATCOM, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

~~(FOUO)~~ Also, JFHQ Kansas did not implement a process to monitor information employees post on the internet. As of February 2012, JFHQ Kansas could not monitor information posted on the internet about JFHQ Kansas (for example, sensitive information or Personally Identifiable Information). JFHQ Kansas had 10 months to correct or mitigate the vulnerability and did not have the resources to contract for the service to monitor information posted on the internet. However, they requested funding for a contract to monitor information posted outside their network. ~~(S//NF)~~ ~~(FOUO)~~

~~(S//NF)~~ JFHQ Kansas should implement a process to monitor information employees post on the internet.

~~(FOUO)~~ Finally, JFHQ Kansas did not implement a process to whitelist Web sites (users only have access to approved Web sites). JFHQ Kansas had 10 months to correct the vulnerability and was still working with the Defense Information Systems Agency to use their Demilitarized Zone Whitelist database to address the recommendation. Whitelisting protects networks by not allowing personnel to access potentially infected or inappropriate Web sites. JFHQ Kansas should implement a process to whitelist Web sites.

~~(FOUO)~~ **377<sup>th</sup> Air Base Wing Did Not Sufficiently Correct or Mitigate Vulnerabilities**

~~(S//NF)~~

OSD/JS, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

OSD/JS, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

~~(S//NF)~~

OSD/JS, STRATCOM, (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

~~(S//NF)~~ OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(e)

[REDACTED]

(FOUO) Also, 377<sup>th</sup> Air Base Wing personnel did not conceal their badges while outside their facilities. 377<sup>th</sup> Air Base Wing personnel had 6 months to correct or mitigate the vulnerability and had performed additional training to mitigate the vulnerability; however, it did not prove effective and was difficult to enforce. [REDACTED]

[REDACTED]. 377<sup>th</sup> Air Base Wing should re-evaluate training on safeguarding Personally Identifiable Information, specifically badges, and perform periodic inspections to determine whether badges are concealed outside of facilities.

(FOUO) As a direct result of 377<sup>th</sup> Air Base Wing personnel not safeguarding their badges, entry guards could not determine [REDACTED]

[REDACTED]. 377<sup>th</sup> Air Base Wing personnel had 6 months to correct or mitigate the vulnerability and had performed additional training for entry guards on allowing access; however, it did not prove effective. As a result, [REDACTED]

[REDACTED] 377<sup>th</sup> Air Base Wing should re-evaluate training for entry guards on identifying false credentials.

(FOUO) Additionally, 377<sup>th</sup> Air Base Wing did not implement the Red Team recommendation to prevent [REDACTED]

[REDACTED]. 377<sup>th</sup> Air Base Wing personnel had 6 months to correct or mitigate the vulnerability and did not determine a solution. 377<sup>th</sup> Air Base Wing personnel were reviewing the process to determine the most practical method of verifying authorizations. Without proper authorization, this allows [REDACTED]

[REDACTED] This would be detrimental to the safety of base occupants and equipment. 377<sup>th</sup> Air Base Wing personnel should approach and require proof of proper restricted area authorization for all persons [REDACTED]

(FOUO) **Unable to Test Two Navy Assessments**

(FOUO) When we attempted to determine if the USS Enterprise and USS George H.W. Bush corrected the vulnerabilities identified in the reports, we were unable to complete the testing. We observed the Navy Red Team attempt to remotely re-assess the USS Enterprise while it was at sea. The Navy Red Team was unable to assess the USS Enterprise network, and we could not validate that the ship addressed its network findings because the testers needed to be physically aboard the ship. The GHWBSG report contained no findings specific to the USS George H.W. Bush; however, the Navy



(FOUO) Red Team provided 10 recommendations in the report. Since the report attributed no findings to the USS George H.W. Bush, we performed no further testing.

(FOUO) **Accountability for Correcting or Mitigating Vulnerabilities**

(FOUO) Overall, the assessed organizations corrected or mitigated 44 of 59 vulnerabilities reported by the Red Teams. JFHQ Kansas and PEO-EIS were the least successful at correcting vulnerabilities. JFHQ Kansas only addressed 5 of 10 vulnerabilities; however, the Red Team did not provide a report to them and responsible JFHQ personnel were unaware of some vulnerabilities. PEO-EIS only addressed one of three vulnerabilities; however, the personnel responsible for tracking and reporting vulnerabilities during the Red Team assessment had left the organization.

(U) **Assessed Organizations Need to Track and Report Vulnerabilities**

(U) DoD organizations should use a Plan of Action and Milestones (POA&M) to track vulnerabilities and should report vulnerabilities to the agency's Inspector General and OMB. Public Law 107-347, "E-Government Act of 2002," Title III, "Federal Information Security Management Act of 2002," December 17, 2002 (FISMA), requires organizations to report significant security weaknesses to OMB. To implement the FISMA, OMB releases memorandums to instruct agencies on how to report security weaknesses. OMB Memorandum M-10-15 and M-11-33 instruct agencies to provide a POA&M to include all security weaknesses found during a vulnerability assessment to the agency's Inspector General and OMB. OMB Memorandum M-04-25 provides the required POA&M elements:

- severity and brief description of weakness,
- responsible party for addressing weakness,
- funding resources required,
- scheduled completion date for resolving weakness,
- key milestones with completion date,
- changes to milestones,
- source of the weakness (how discovered), and
- status of corrective actions.

(U) NSA and the Navy follow OMB guidance to implement FISMA reporting. The Army implemented FISMA using AR 25-1, "Army Knowledge Management and Information Technology," December 4, 2008. This guidance requires all Army organizations to report vulnerabilities in accordance with FISMA. The Air Force implemented FISMA using Air Force Instruction (AFI) 33-210, "Air Force Certification and Accreditation (C&A) Program (AFCAP)," December 23, 2008; and AFI 33-200, "Information Assurance (IA) Management," October 15, 2010. The guidance states that the Enterprise Information Technology Data Repository, which is the primary source for FISMA data reporting, includes vulnerability reporting. Additionally, the guidance designates the Secretary of the Air Force, Network Services Directorate as the responsible party to manage the annual assessment of the Air Force Information

(U) Assurance Programs as required by FISMA. This allows the Air Force Senior Information Assurance Officer to answer the annual FISMA report questions posed by OMB. However, the six assessed organizations did not comply with Federal and DoD guidance for tracking and reporting security weaknesses.

~~(FOUO)~~ For six assessed organizations, we requested the POA&Ms and evidence of security weaknesses reporting in accordance with FISMA, OMB, or local guidance. The six assessed organizations were unable to provide evidence that the organizations reported the vulnerabilities found by the Red Team.

~~(FOUO)~~ Three of the six assessed organizations (NSA, JFHQ Kansas, and USS Enterprise of the ENTSG) did not create a POA&M. Three organizations created POA&Ms; however, the BIMA POA&M did not include all of the OMB required elements, and was not updated when weaknesses were addressed until our site visit, which was over a year after the assessment date. The PEO-EIS created the POA&M after the DoD OIG site visit, which was over a year after the assessment date. The 377<sup>th</sup> Air Base Wing created a POA&M, but did not include all of the OMB required elements. Table 4 provides a summary of the tracking and reporting of security weaknesses and identifies the following: the assessed organization and the Red Team that assessed them, the total number of security weaknesses/vulnerabilities identified for each organization, whether the assessed organization created a POA&M to track the security weaknesses, and the number of security weaknesses the assessed organization reported.

~~(FOUO)~~ Table 4. Unreported Security Weaknesses

Assessed Organization*	Security Weaknesses Identified	POA&M Created	Security Weakness Reported
<del>(FOUO)</del> NSA (b)(3)			
BIMA by Army Red Team	15	Yes- But the POA&M did not contain milestone dates, and was not updated until our site visit.	None
PEO-EIS by Army Red Team	3	Yes- But PEO-EIS created the POA&M after our site visit and over a year after the Red Team assessment	None
JFHQ by Air Force Red Team	10	No	None
377 <sup>th</sup> Air Base Wing by Air Force Red Team	28	Yes- But the POA&M did not contain milestone dates	None
USS Enterprise of the ENTSG by Navy Red Team	3	No	None

\* ~~(FOUO)~~ The GHWBSG report had no security weaknesses specific to the USS George H.W. Bush to track or report.

(FOUO) NSA (b)(3) [REDACTED]

(FOUO) The other organizations, BIMA, PEO-EIS, JFHQ Kansas, and the 377<sup>th</sup> Air Base Wing did not create or appropriately create POA&Ms or report vulnerabilities because officials incorrectly viewed the assessment as an internal operation that did not require additional reporting. Since the officials viewed the assessments as internal operations, they determined that the results of the assessments did not need to be tracked or reported. BIMA, PEO-EIS, JFHQ Kansas, and the 377<sup>th</sup> Air Base Wing should track and report vulnerabilities in accordance with OMB requirements.

(FOUO) As a result, the assessed organizations did not have a fully effective vulnerability management program. Reporting security weaknesses assists in building a defensible enterprise for protecting agency information and information systems.

(U) **Conclusion**

(FOUO) The assessed organizations did not correct or mitigate, appropriately track with a POA&M, or report all security weaknesses. Consequently, unnecessary risk exists on DoD networks. Specifically, this could result in:

DoDIG (b)(7)(E) [REDACTED]

(FOUO) Unauthorized individuals could exploit vulnerabilities to [REDACTED] DoDIG (b)(7)(E)

**(U) Management Comments on the Finding and Our Response**

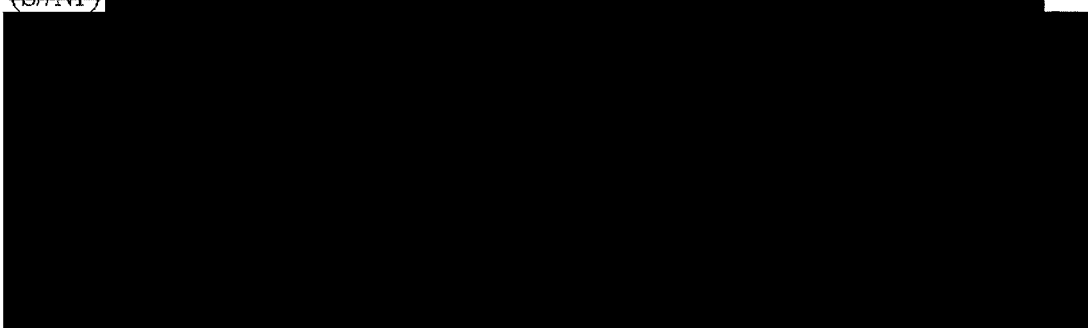
**(U) *Biometrics Identity Management Agency Comments on Correcting or Mitigating Vulnerabilities***

~~(S//NF)~~ OSD//IS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(e)



**(U) *Our Response***

~~(S//NF)~~ OSD//IS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(e)



**(U) Recommendations, Management Comments, and Our Response**

**(U) *Revised Recommendations***

~~(FOUO)~~ As a result of management comments, we revised draft Recommendation B.1 to clarify the corrective actions are specific to the respective organization. Also, we revised Recommendations B.1. and B.2. to include Chief before Central Security Service.

NSA (b)(3)



~~(FOUO)~~ B.1. We recommend that the

NSA (b)(3)



(U) **National Security Agency/Central Security Service Comments**

(U) The Director, NSA/Chief, Central Security Service, agreed with the recommendation and suggested verbiage to clarify the recommendation is for the DoD Components to develop such policy for the systems for which they have responsibility.

(U) **Our Response**

(U) Although the Director, NSA/Chief, Central Security Service, agreed with the recommendation, the comments were not responsive. He did not include corrective actions. We request the Director provide corrective actions in response to the final report.

(U) **Management Comments Required**

(U) The Adjutant General, JFHQ Kansas, did not comment on Recommendation B.1. We request the Adjutant General provide comments in response to the final report.

(U) **Biometrics Identity Management Agency Comments**

~~(S//NF)~~

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

(U) **Our Response**

(U) Comments from the Deputy were responsive and met the intent of our recommendation. Therefore, no further comments are required.

(U) **Program Executive Office-Enterprise Information Systems Comments**

(U) The Deputy Program Executive Officer, Enterprise Information Systems, responding on behalf of the Program Executive Officer, Enterprise Information Systems, neither agreed nor disagreed and stated PEO-EIS have a C&A policy in place for reporting and resolving security weaknesses using the POA&M process. Also, the Regional Computer Emergency Response Team added the PEO-EIS Information Assurance Program Manager to the distribution lists for all persistent security tests.

(U) **Our Response**

(U) Comments from the Deputy were responsive and met the intent of our recommendation. Therefore, no further comments are required.

**(U) Management Comments Required**

(U) The Commander, 377<sup>th</sup> Air Base Wing, did not comment on the draft of this report. We request that the Commander provide comments in response to the final report.

~~(FOUO)~~ **B.2. We recommend that the**

NSA (b)(3), STRATCOM (b)(1), Sec. 1.7(e)

**(U) National Security Agency/Central Security Service Comments**

~~(FOUO)~~ The Director, NSA/Chief, Central Security Service, agreed with the recommendation and suggested verbiage to clarify the recommendation.

**(U) Our Response**

(U) Although the Director, NSA/Chief, Central Security Service, agreed with the recommendation, the comments were not responsive. The Director did not include corrective actions. We request the Director provide corrective actions in response to the final report.

~~(FOUO)~~ B.3. We recommend that the Commander, U.S. Fleet Forces Command, in coordination with the USS George H. W. Bush Strike Group and the USS Enterprise Strike Group, implement, track, and validate that a Plan of Actions and Milestones has been created and verify that all security weaknesses are reported.

**(U) Management Comments Required**

(U) The Commander, USFLTFORCOM, did not comment on the draft of this report. We request that the Commander provide comments in response to the final report.

~~(FOUO)~~ **B.4. We recommend that the Adjutant General, Joint Forces Headquarters Kansas, implement, track, and validate that a Plan of Actions and Milestones has been created to correct the outstanding vulnerabilities for misconfigured software, inputting and storing sensitive information on NIPRNET, unsecure password configurations, monitoring employee information posted outside of the Joint Forces Headquarters Kansas network, and restricting access to Web sites and verify that all security weaknesses are reported.**

**(U) Joint Forces Headquarters, Kansas Comments**

(U) The CIO/Director of Information Management, JFHQ Kansas, responding on behalf of the Adjutant General, Joint Forces Headquarters, partially agreed with the recommendation. The CIO/Director of Information Management stated corrective actions had been implemented for the first three items. The CIO/Director of Information Management disagreed on the last two items. He stated the Public Web content is a Public Affairs function. Public Affairs approves content for official Web pages and official media sites, and receives alerts when key words concerning the Kansas National

(U) Guard are posted. He stated that since the Kansas systems resided on the National Guard Bureau domain, all internet traffic is routed through the National Guard Bureau routers and firewalls. Finally, he stated the National Guard Bureau maintained a Web cache that controls access to unauthorized sites.

(U) ***Our Response***

(U) Although the CIO/Director of Information Management only partially agreed, the comments were responsive and corrective actions met the intent of the recommendation. Therefore, no further comments are required.

~~(FOUO)~~ **B.5. We recommend that the Director, Biometrics Identity Management Agency, implement, track, and validate that a Plan of Actions and Milestones has been created to correct the outstanding vulnerabilities for safeguarding Personally Identifiable Information, establishing a wireless policy that determines which logs to maintain, defines threat level of activity (for example, severe, critical, major, minor, and safe), and defines actions to perform based on severity of activity, and**  
~~STRATCOM (b)(1), Sec. 1.7(e)~~ [REDACTED] **and verify that all security weaknesses are reported.**

(U) ***Biometrics Identity Management Agency Comments***

~~(S//NF)~~ ~~(S//NF)~~ ~~(S//NF)~~ ~~OSD/JS (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)~~  
[REDACTED]

(U) ***Our Response***

(U) Comments from the Deputy were responsive and met the intent of our recommendation. Therefore, no further comments are required.

~~(FOUO)~~ **B.6. We recommend that the Program Executive Officer, Enterprise Information Systems, implement, track, and validate that a Plan of Actions and Milestones has been created to correct the outstanding vulnerabilities for**  
~~STRATCOM (b)(1), Sec. 1.7(e)~~ [REDACTED] **and verify that all security weaknesses are reported.**

(U) ***Program Executive Office-Enterprise Information Systems Comments***

~~(S//NF)~~ ~~(S//NF)~~ ~~(S//NF)~~ ~~OSD/JS (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)~~  
[REDACTED]

~~(S//NF)~~ OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)  
~~(S//NF)~~

(U) ***Our Response***

(U) Comments from the Deputy were responsive and met the intent of our recommendation. Therefore, no further comments are required.

~~(FOUO)~~ B.7. We recommend that the Commander, 377<sup>th</sup> Air Base Wing, implement, track, and validate that a Plan of Actions and Milestones has been created to correct the outstanding vulnerabilities for ~~STRATCOM (b)(1), Sec. 1.7(e)~~ safeguarding Personally Identifiable Information, identifying false credentials used to gain installation access, and controlling actions in restricted areas and verify that all security weaknesses are reported.

(U) **Management Comments Required**

(U) The Commander, 377<sup>th</sup> Air Base Wing, did not comment on the draft of this report. We request that the Commander provide comments in response to the final report.



(U) **Finding C. Improvements Needed for the C&A Process**

~~(FOUO)~~ NSA: (b)(3) [Redacted]

NSA: (b)(3) [Redacted]

~~(FOUO)~~ NSA: (b)(3) [Redacted]

(U) **C&A Process Did Not Include a Review of Proficiency, Training, and Certification**

~~(S//REL USA, FVEY)~~ OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g) [Redacted]

(FOUO)

NSA: (b)(3)

[Redacted]

(FOUO)

NSA: (b)(3)

[Redacted]

[Redacted]

**(U) C&A Process Needs to Evaluate the Proficiency of Red Team Members**

(S//REL USA, FVEY)

OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

[Redacted]

OSD/JS (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)

[Redacted]

(FOUO)

NSA: (b)(3)

[Redacted]

NSA: (b)(3)

[Redacted]

**(U) C&A Process Needs to Evaluate Training and Certifications of Red Team Members**

~~(FOUO)~~ NSA (b)(3)  
[Redacted]

**(U) NSA Needs to Validate Proficiency of the Red Teams**

~~(FOUO)~~ NSA (b)(3)  
~~(FOUO)~~ NSA (b)(3)  
[Redacted]

**~~(FOUO)~~ Air Force Red Team Certification Vote Did Not Have a Quorum**

~~(FOUO)~~ NSA (b)(3)  
[Redacted]

~~(FOUO)~~ NSA (b)(3)  
[Redacted]

~~(FOUO)~~ NSA: (b)(3)  
[Redacted]

~~(FOUO)~~ NSA: (b)(3)  
[Redacted]

~~(FOUO)~~ NSA: (b)(3)  
[Redacted]

~~(FOUO)~~ NSA: (b)(3)  
[Redacted]

~~(FOUO)~~ NSA: (b)(3)  
[Redacted]

**(U) Conclusion**

~~(S//REL USA, FVEY)~~ NSA: OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g), NSA: (b)(3)  
[Redacted]

<sup>8</sup> ~~(FOUO)~~ The application package consists of a letter of request, self-assessment results, completed application checklist, and all required documentation for the Evaluators Scoring Metrics.

~~(S//REL USA, FVEY)~~

NSA: OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g); NSA: (b)(3)

~~(S//REL USA, FVEY)~~

NSA: OSD/JS: STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g); NSA: (b)(3)

## (U) Recommendations, Management Comments, and Our Response

### (U) *Revised Recommendations*

~~(FOUO)~~ As a result of management comments, we revised draft Recommendation C.1. to include Chief before Central Security Service.

~~(FOUO)~~ C.1.

NSA: (b)(3)

a. Establish a process in accordance with DoD Instruction O-8530.2, "Computer Network Defense (CND)," March 9, 2001, and the Chairman of the Joint Chiefs of Staff "Execute Order to Incorporate Realistic Cyberspace conditions into Major Exercises," February 11, 2011, for the Certification Board to evaluate Red Team qualifications to perform their mission functions and activities.

### (U) *U.S. Strategic Command Comments*

~~(S//REL USA, FVEY)~~

NSA: OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g); NSA: (b)(3)

### (U) *Our Response*

~~(S//REL USA, FVEY)~~

NSA: OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g); NSA: (b)(3)

(U) **National Security Agency/Central Security Service Comments**

~~(FOUO)~~ NSA: (b)(3)

(U) **Our Response**

(U) Comments from the Director were responsive. No further comments are required.

b. ~~(FOUO)~~ **Implement Certification and Accreditation procedures to incorporate Red Team qualification, training, and certifications in the Certification decision as required by DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," April 23, 2007.**

(U) **U.S. Strategic Command Comments**

~~(S//REL USA, FVEY)~~ NSA: OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(e); NSA: (b)(3)

(U) **Our Response**

~~(S//REL USA, FVEY)~~ OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(e)

(U) **National Security Agency/Central Security Service Comments**

~~(FOUO)~~ NSA: (b)(3)

(U) **Our Response**

(U) Although the Director, NSA/Chief, Central Security Service, agreed with the recommendation, the comments were not responsive. The Director did not provide corrective actions. We request the Director provide corrective actions in response to the final report.

(U) **U.S. Fleet Cyber Command/U.S. Tenth Fleet Comments**

~~(FOUO)~~ Although not required to comment, the Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet agreed with Recommendations C.1.a and C.1.b and stated the C&A process is heavily focused on the administrative aspects of Red Teams. The Commander stated the process needs to be expanded to include assessing Red Team operational proficiency and capability to meet mission objectives. This should include periodic C&A observations during Red Team operations.

(U) **Our Response**

(U) We agree with the intent of the Commander's comments.

c. (FOUO) NSA: (b)(3)



(U) **U.S. Strategic Command Comments**

(U) The Director, C4 Systems, responding on behalf of the Commander, USSTRATCOM, stated The NSA Handbook will be replaced with CJCS Manual 6510.03, "Department of Defense (DoD) Cyber Red Team Certification and Accreditation (C&A)," which requires the evaluation team to consist of at least six members and any deviations from the requirements of the Manual must be coordinated through the Certification Authority and approved by the Accrediting Authority. In addition, through further correspondence the Chief, Cybersecurity Assurance Division, responding on behalf of the Commander, USSTRATCOM, agreed with the recommendation.

(U) **Our Response**

(U) Comments from the Director were responsive. No further comments are required.

(U) **National Security Agency/Central Security Service Comments**

(U) The Director, NSA/Chief, Central Security Service, agreed and stated the NSA Red Team will adhere to the quorum requirement.

(U) **Our Response**

(U) Although the Director, NSA/Chief, Central Security Service, agreed with the recommendation, the Director's comments were only partially responsive. While the Director stated the NSA Red Team will follow the quorum requirement, he did not state NSA will develop procedures for any deviations from the established procedures to be formally documented and approved. We request that the Director provide additional comments in response to the final report.

**d. (FOUO) Review and evaluate the 57<sup>th</sup> Information Aggressor Squadron and the 177<sup>th</sup> Information Aggressor Squadron as separate Red Teams for Certification and Accreditation.**

(U) **U.S. Strategic Command Comments**

(U) The Director, C4 Systems, responding on behalf of the Commander, USSTRATCOM, stated USSTRATCOM/U.S. Cyber Command will work with the NSA Red Team to schedule an onsite evaluation of the 177<sup>th</sup> IAS. In addition, through further correspondence the Chief, Cybersecurity Assurance Division, responding on behalf of the Commander, USSTRATCOM, agreed with the recommendation.

**(U) Our Response**

(U) Comments from the Director were partially responsive. The Director did not address the 57<sup>th</sup> IAS receiving an onsite evaluation separate from the 177<sup>th</sup> IAS. We request the Director provide comments in response to the final report.

**(U) National Security Agency/Central Security Service Comments**

(U) The Director, NSA/Chief, Central Security Service, agreed and stated they will determine a new evaluation date once the C&A qualification for Red Teams is revised.

**(U) Our Response**

(U) Comments from the Director were partially responsive. We request that the Director provide a timeframe for performing the evaluation.

e. ~~(FOUO)~~ **Review the validity of the Red Team Accreditation letter given to the 57<sup>th</sup> Adversary Tactics Group.**

**(U) U.S. Strategic Command Comments**

(U) The Director, C4 Systems, responding on behalf of the Commander, USSTRATCOM, stated USSTRATCOM/U.S. Cyber Command will work with the NSA Red Team to schedule an onsite evaluation of the 177<sup>th</sup> IAS, and USSTRATCOM will provide updated accreditation letters for the 57<sup>th</sup> ATG and 177<sup>th</sup> IAS, as appropriate, based on the outcome of the evaluations. In addition, through further correspondence the Chief, Cybersecurity Assurance Division, responding on behalf of the Commander, USSTRATCOM, agreed with the recommendation.

**(U) Our Response**

(U) Comments from the Director were responsive. No further comments are required.

**(U) National Security Agency/Central Security Service Comments**

(U) The Director, NSA/Chief, Central Security Service, agreed and stated the letter should be revised, if needed, and written to the specific organization being evaluated.

**(U) Our Response**

(U) Comments from the Director were responsive. No further comments are required.



## (U) Appendix A. Scope and Methodology

(U) We conducted this performance audit from July 2011 through September 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

~~(FOUO)~~ We reviewed the Red Teams' reporting process, the effectiveness of Red Teams' reports, and the Red Team C&A process. Specifically, we visited:

- USSTRATCOM at Offutt Air Force Base, Nebraska;
- U.S. Cyber Command at Fort Meade, Maryland;
- NSA Red Team at Fort Meade, Maryland;
- U.S. Army Red Team at Fort Belvoir, Virginia;
- U.S. Navy Red Team at Naval Station Norfolk, Virginia;
- U.S. Air Force Red Teams at McConnell Air Force Base, Kansas and Nellis Air Force Base, Nevada; and
- U.S. Marine Corps Red Team at Quantico Marine Corps Base, Virginia.

### (U) Red Team Missions Selected for Review

~~(FOUO)~~ We selected seven Red Team missions to determine whether Red Teams identified and reported the vulnerabilities found during assessments; and whether the assessed organizations corrected or mitigated, tracked, and reported the vulnerabilities identified during Red Team assessments. The Red Team missions we selected are as follows:

- ~~(FOUO)~~ NSA (b)(3) [REDACTED]
- Army Red Team – “Biometrics Identity Management Agency and the Automated Biometric Information System, Clarksburg, WV Red Vulnerability Assessment Report,” November 28, 2010;
- Army Red Team – “1<sup>st</sup> Cavalry Division Fort Hood, TX Red Vulnerability Assessment Report”;<sup>1</sup>
- Navy Red Team – “Cyber Defense Assessment Team Activity Report for USS Enterprise Strike Group Joint Task Force Exercise 11-2,” January 6, 2011;
- Navy Red Team – “Cyber Defense Assessment Team Activity Report for USS George H.W. Bush Strike Group Joint Task Force Exercise 11-4,” March 17, 2011;<sup>2</sup>

---

<sup>1</sup> (U) We did not assess the 1<sup>st</sup> Cavalry Division Fort Hood, Texas mission. The 1<sup>st</sup> Cavalry Division SIPRNET was disconnected because the personnel responsible for the network were deployed overseas during the audit period.

<sup>2</sup> (U) We did not assess the USS George H.W. Bush because no findings were attributed to the ship in the report.

- ~~(FOUO)~~ Air Force Red Team – “Mobile Training Team Final Report, Kirtland Air Force Base,” July 7, 2011; and
- Air Force Red Team – Joint Forces Headquarters, Topeka, Kansas.<sup>3</sup>

(U) Specifically, we:

- Interviewed Red Team members to discuss the reports selected and discussed the Red Team’s methodology and objectives for the assessments so the audit team could re-evaluate if the assessed organizations had appropriately corrected or mitigated the vulnerabilities. Additionally, we reviewed the Rules of Engagement for the agreed upon mission parameters, including network boundaries, halting conditions, reconnaissance objectives, exploitation objectives, mission specific requirements, and reporting.
- Developed a test plan to assess the findings in the reports; developed testing procedures in conjunction with the Technical Assessment Directorate (TAD) to validate if the assessed organizations properly mitigated the findings identified by the Red Team.
- Interviewed the assessed organizations to verify that they corrected or mitigated, tracked, and reported physical and network security findings.
- We inquired if the assessed organizations were aware of the requirements of FISMA and OMB to create a POA&M and report all security weaknesses. We verified if the assessed organizations properly reported security weaknesses identified as required by FISMA and local service regulations AR 25-1, AFI 33-200, and AFI 33-210. Additionally, we requested the POA&Ms to determine if the assessed organizations corrected or mitigated and tracked the vulnerabilities found by the Red Team.
- Tested the vulnerabilities with the assessed organizations and determined whether they had implemented proper mitigation actions. This included a walkthrough of physical security procedures as well as verification of network vulnerability mitigation.

### (U) **Red Team C&A Process Review**

(U) We reviewed the Red Team’s Certification and Accreditation packages and assessment process to determine the effectiveness of their evaluation and scoring metrics. We assessed whether the Certification and Accreditation process effectively reviews the Red Teams’ qualifications and expertise to conduct operations. Specifically, we:

- Interviewed Red Team members at the following locations: NSA, Army, Air Force, Navy, and Marine Corps to determine the requirements for obtaining Certification and Accreditation for becoming a Red Team.
- Obtained, reviewed, and analyzed the C&A packages of each Red Team (NSA, Army, Air Force, and Navy). C&A packages included: The Certification Letter

---

<sup>3</sup> (U) Air Force Red Team did not produce a report.

(U) including NSA's recommendation for Accreditation, Evaluator's Scoring Metrics, SOPs, and USSTRATCOM's Accreditation Letter.

- Evaluated the C&A Packages from each of the Red Teams using the evaluation criteria in NSA's Draft "Evaluator Handbook for Red Team Certification and Accreditation," June 17, 2010.
- Interviewed USSTRATCOM and NSA personnel regarding their role in the C&A process.
- Requested and reviewed supporting documentation such as Red Team SOPs, Red Team missions, or Red Team guidance to determine how each Red Team functions.

### (U) **Use of Computer-Processed Data**

(U) We did not rely on computer-processed data to perform this audit.

### (U) **Use of Technical Assistance**

(U) The DoD OIG Quantitative Methods Directorate (QMD) assisted with the audit. Based on QMD's recommendation the audit team used a non-statistical sample to select seven Red Team assessments performed from July 2010 through June 2011 by the NSA Red Team, Army Red Team, Air Force Red Team, and Navy Red Team for audit review. In addition, QMD provided instructions for control testing sampling. We used a sampling plan with a 90-percent confidence level and an upper bound of 5 percent. We

NSA: (b)(3)

(U) TAD also assisted with the audit, using their expertise in verifying whether the assessed organizations appropriately corrected or mitigated network-specific vulnerabilities identified by the Red Teams.

(U) Specifically, the audit team along with TAD:

- Reviewed the NSA & Service Components' assessment reports and other related documents.
- Developed a test plan based on NSA & Service Components' recommendations.
- Requested the assessed organizations' personnel for the demonstration of controls based on TAD test plan.

### (U) **Prior Coverage**

(U) No prior coverage has been conducted on the subject during the last 5 years.

## (U) Appendix B. Supplemental Background Information

(FOUO) There are five Red Teams in the DoD that have been certified and accredited as of August 5, 2011. The table below provides an overview of the accredited Red Teams and identifies the following: the accredited Red Teams, their mission, and their headquarters location.

### (U) List of Accredited Red Teams With Mission

Accredited Red Teams	Red Team Mission	Headquarters
National Security Agency Red Team	The NSA Red Team performs assessments on the DoD, other Federal Government agencies, and Intelligence Community, as well as COCOM exercises with the other DoD Red Teams.	Fort Meade, Maryland
Army Red Team – 1 <sup>st</sup> Information Operations Command	The Red Team conducts full spectrum information warfare assessments as an independent opposing force. They use both active and passive capabilities to expose and exploit information operations vulnerabilities of friendly forces to improve the security posture and readiness of DoD components.	Fort Belvoir, Virginia
Navy Red Team – Navy Information Operations Command	The Red Team mission is to fulfill requirements in support of Naval forces afloat and ashore, as well as support all COCOM operations and exercises.	Naval Station Norfolk, Virginia
Air Force Red Team – 57 <sup>th</sup> ATG	The Red Team mission is to train USAF joint and allied personnel by replicating current and emerging threats as a professional information opposing force.	57 <sup>th</sup> IAS – Nellis Air Force Base, Nevada & 177 <sup>th</sup> IAS – Mc Connell Air Force Base, Kansas
Marine Corps Red Team – Marine Corps Information Assurance Red Team	The Red Team mission is to demonstrate the effects of a network compromise so Marine Corps leadership better understands the significance of information security and assurance programs.	Quantico Marine Corps Base, Virginia

(S//REL USA, FVEY)

OSD/JS: STRATCOM (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

<sup>4</sup> (U) Combatant commands involved in FY11 Director, Operational Test and Evaluation exercises- Africa Command, Central Command, European Command, Joint Forces Command, Northern Command, Pacific Command, Southern Command, Special Operations Command, Strategic Command, and Transportation Command.

~~(S//REL USA, FVEY)~~

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

(U) The Director, Operational Test and Evaluation combines the results of all the combatant command exercises and reports them to Congress annually.

~~(S//REL USA, FVEY)~~

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

~~(S//REL USA, FVEY)~~

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

~~(S//REL USA, FVEY)~~

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

---

<sup>5</sup> (U) White Team - acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission

## (U) **Appendix C. Federal and DoD Guidance**

(U) We used the following guidance throughout the audit.

### (U) **OMB Guidance**

(U) OMB Memorandum M-11-33, "FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," September 14, 2011, provides instructions for agency's FY 2011 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). The goal for Federal information security in FY 2011 is to build a defensible Federal enterprise that enables agencies to harness technological innovation, while protecting agency information and information systems.

(U) OMB Memorandum M-10-15, "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," April 21, 2010, instructs agencies to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way to meet the reporting requirements for FISMA.

(U) OMB Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004, provides updated instructions for agency reporting under the FISMA Act of 2002.

### (U) **FISMA of 2002**

(U) Public Law 107-347, "E-Government Act of 2002," Title III, "Federal Information Security Management Act of 2002," December 17, 2002, provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

### (U) **Committee on National Security Systems**

(U) Committee on National Security Systems Instruction 4009, "National Information Assurance (IA) Glossary," April 26, 2010, is a glossary that is for individuals that collect, generate, process, store, display, transmit, or receive classified or sensitive information or that operate, use, or connect to National Security Systems.

### (U) **CJCS Guidance**

(U) CJCS Instruction 6510.01E, "Information Assurance (IA) and Computer Network Defense (CND)," August 12, 2008, provides joint policy and guidance for Information Assurance and CND operations. The Instruction provides Joint Staff, COCOMs, Services, Defense agencies, DoD field activities IA and CND responsibilities for Red Team operations, vulnerability, and incident response assessment coordination.

(U) CJCS Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, provides joint policy and responsibilities for Information Assurance and support to CND. The Instruction provides Joint Staff,

(U) COCOMs, Services, Defense agencies, DoD field activities, and Joint Activities responsibilities for Cyber Security Inspection Program.

~~(S//REL TO USA, FVEY)~~

OSDJS, STRATCOM: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)

### (U) DoD Guidance

(U) DoD Directive 8500.01E, "Information Assurance (IA)," certified current as of April 23, 2007, establishes policy and assigns responsibilities to achieve DoD information assurance (IA). Specifically, DoDD 8500.01E directs organizations to track and mitigate vulnerabilities.

(U) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, implements the policies outlined in DoDD 8500.01E by implementing policy, assigning responsibilities, and prescribing procedures for applying integrated, layered protection of the DoD information systems and networks. This document lists the subject area, control number, and a brief explanation of each mission assurance category controls for integrity and availability. The following subject area controls are defined by the DoD I 8500.2, are as follows: Security Design and Configuration, Identification and Authentication, Enclave and Computing Environment, Enclave Boundary Defense, Physical and Environmental, Personnel, Continuity, Vulnerabilities and Incident Management.

~~(FOUO)~~ DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001, establishes computer network defense policy, and responsibilities necessary to provide the essential structure and support to the Commanders USSTRATCOM for computer network defense within DoD information systems and computer networks.

~~(FOUO)~~ DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001, Implements policy, assigns responsibilities, and prescribes procedures necessary to provide the essential structure and support to the U.S. Space Command for CND within DoD information systems and computer networks. This Instruction also provides for Information Assurance Red Team notification, reporting and coordination to insure deconfliction of Red Team and CND activities. U.S. Space Command has been disestablished; their responsibilities were assigned to USSTRATCOM.

(U) DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," certified current as of April 23, 2007, establishes policy and assigns responsibilities for DoD information assurance training, certification and workforce management. The Directive provides the Director, National Security Agency, direction and control of the Under Secretary of Defense for Intelligence to implement, in

(U) coordination with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO) and DoD Components, as appropriate a certification program for Red Teams and Vulnerability Assessment Teams. ASD (NII) has been disestablished and their responsibilities transferred to the DoD CIO.

### (U) **Army Regulations**

(U) AR 25-1, "Army Knowledge Management and Information Technology," December 4, 2008, states Army should comply with FISMA.

(U) AR 380-53, "Communication Security Monitoring," December 23, 2011, sets forth policies, responsibilities, and procedures for conducting communications security monitoring, information operations Red Team activities, and Computer Defense Association Program activities within the Army and in support of Joint and combined operations and activities. Specifically, it states that Red Team findings are reportable only to the unit requesting the assessment. The requesting unit must authorize distribution of the Red Team vulnerability assessment report to parties other than the requesting unit.

(U) Army Best Business Practice 09-EC-M-0010, "Wireless Security Standards," version 3.0, January 2, 2009, requires broadcast option for the Extended Service Set Identifier or Service Set Identifier, which is used in determining the authorized group of mobile radios, to be turned off at the Wireless Access Point.

### (U) **Air Force Instructions**

(U) AFI 33-200, "Information Assurance (IA) Management," October 15, 2010, requires the Secretary of the Air Force, Network Services Directorate to provide detailed information on the FISMA requirements via the annual Air Force FISMA Reporting Guidance. The Secretary of the Air Force, Network Services Directorate is required to manage the annual assessment of the Air Force Information Assurance Programs as required by FISMA. This allows the Air Force Senior Information Assurance Officer to answer the annual FISMA report questions posed by OMB.

(U) AFI 33-210, "Air Force Certification and Accreditation (C&A) Program (AFCAP)," December 23, 2008, states that IAMs will conduct a review of all applicable IA controls and perform validation procedures on those controls as identified in the annual FISMA reporting requirements. The Enterprise Information Technology Data Repository is the primary source for FISMA data reporting.



## (U) **Glossary**

(U) **Accreditation** - Formal declaration by the Designated Approving/Accrediting Authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

(U) **Basic Input/ Output System** - The BIOS is a program built into personal computers that starts the operating system when the user turns the computer on. BIOS is part of the hardware of the computer and is separate from the operating system.

(U) **Certification** - Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

(U) **Computer Network Defense** - Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. Note: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, and detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, for example, network operations, CND Services, intelligence, counterintelligence, and law enforcement. CND response can include recommendations or actions by network operations (including information assurance) restoration priorities, law enforcement, military forces and other U.S. Government agencies.

(U) **Cybersecurity** - The ability to protect or defend the use of cyberspace from cyber attacks.

(U) **Cyberspace** - A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

(U) **Intrusion Detection System** - Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

(U) **Red Team** - An independent threat based activity aimed at readiness improvements through simulation of an opposing force. Red teaming activity includes becoming knowledgeable of a target system, matching an adversary's approach, gathering appropriate tools to attack the system, training, launching an attack, then working with system owners to demonstrate vulnerabilities and suggest countermeasures.

(U) **Spillage** - Security incident that results in the transfer of classified or Controlled Unclassified Information onto an information system not accredited (for example authorized) for the appropriate security level.

(U) **Spoofing** - 1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action.

(U) **Strike Group** - A Strike Group (officially called a Carrier Strike Group but referred to by the Navy as a Strike Group) is a group of U.S. Navy ships typically comprised of an aircraft carrier, guided missile cruiser, two guided missile destroyers, attack submarine, and a combined ammunition, oiler, and supply ship.

(U) **Vulnerability Assessment** - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

(U) **War Games** - A simulation, by whatever means, of a military operation involving two or more opposing forces, using rules, data, and procedures designed to depict an actual or assumed real-world situation.

(U) **Whitelist** - A filter used to limit interactions to trusted sources. The filter is set to access only trusted sites while blocking all others.

(U) **White Team** - Act as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results.

# Department of the Army Comments

Final Report  
Reference



DEPARTMENT OF THE ARMY  
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2  
1000 ARMY PENTAGON  
WASHINGTON, DC 20310-1000

DAMI-CDS

31 OCT 2012

*8 11/12/12*  
MEMORANDUM THRU ASSISTANT DEPUTY CHIEF OF STAFF, G-2, 1000 ARMY PENTAGON, WASHINGTON, DC 20310-1596

FOR DEPUTY INSPECTOR GENERAL FOR AUDITING, READINESS, OPERATIONS AND SUPPORT, 4300 MARK CENTER DRIVE, ALEXANDRIA, VA 22350-1500

SUBJECT: DoDIG Draft Report for Comment - Better Reporting and Coordination Processes Can Improve Red Teams Effectiveness.

1. Reference memorandum, DoDIG, 28 Sep 12, subject: DoDIG Draft Report for Comment - Better Reporting and Coordination Processes Can Improve Red Teams Effectiveness
2. The Office of the Deputy Chief of Staff (ODCS), G-2 reviewed recommendation A.1 and concurs with the DoD Inspector General's recommendation to revise AR 380-53 to not limit distribution of Red Team reports to only the assessed organizations, but distribute Red Team reports to the appropriate DoD components in accordance with CJCSI 6510.01F.
3. In order to comply, the ODCS, G-2 (Technical Security Branch) provided notification to the Army Publishing Directorate (APD) of the requested change. APD is currently working to publish an administrative revision to incorporate the policy change to reflect the requirements of CJCSI 6510.01F.
4. The ODCS, G-2 point of contact is [REDACTED]

*Gerry B. Turnbow*  
GERRY B. TURNBOW  
Director, Counterintelligence, Human  
Intelligence, Disclosure & Security

# U.S. Strategic Command Comments

Final Report  
Reference



~~SECRET//NOFORN USA, FVEY~~  
DEPARTMENT OF DEFENSE  
UNITED STATES STRATEGIC COMMAND

Reply To:  
USSTRATCOM/J6  
901 SAC BLVD STE 2B9  
OFFUTT AFB NE 68113-6600

NOV 06 2012

MEMORANDUM FOR THE OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Subject: (U) USSTRATCOM Response to DoD OIG Project No. D2011-D0001C-0747 000

1. (U) References:

a. (U) DoD IG Project No. D2011-D0001C-0247 000, *Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness*, 28 September 2012.

b. (U) USSTRATCOM Execute Order: *Incorporate Realistic Cyberspace Conditions Into Major DoD Exercises (SIREL USA, FVEY)*, 28 March 2011.

2. (U) In accordance with reference a, the USSTRATCOM Cyber Red Team Accrediting Authority provides the following response:

a. ~~(U//FOUO)~~ DoD OIG Recommendation: We recommend the Commander, U.S. Strategic Command, develop a standard report format for Red Teams in accordance with the Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," 9 February 2011.

(U) USSTRATCOM Response: Commander, United States Cyber Command (CDRUSCYBERCOM) tasked in paragraph 3.C.1.1 of reference b with development of a standard reporting tool to capture lessons learned, including effective responses to Red Team actions, disseminating updates annually in the Global Cyber-Synchronization Conference, or more frequently, as needed, and sharing lessons learned from Red Team operations with Combatant Commands, Components, Computer Network Defense Service Providers, and Director, Operational Test & Evaluation in order to improve global cyber defenses. Additionally, USSTRATCOM/USCYBERCOM will work with the National Security Agency (NSA) Cyber Red Team to develop/disseminate a standard report format.

Classified By: [REDACTED], USSTRATCOM/J3  
Reason: 1.4(a)  
Declassify on: ~~28 March 2036~~

~~SECRET//NOFORN USA, FVEY~~

~~SECRET//NOFORN~~

b. ~~(S)~~ DoD OIG Recommendation: We recommend the Commander, USSSTRATCOM, and the Director, NSA/Central Security Service, coordinate to:

(1) (U) Establish a process in accordance with DoD Instruction O-8530.2, "Computer Network Defense (CND)," 9 March 2001, and the ~~(S)~~ <sup>OSD/JS, STRATCOM (b)(1), Sec. 1.7(e)</sup>

February 2011, for the Certification Board to evaluate Red Team qualifications to perform their mission functions and activities.

(2) (U) Implement Certification and Accreditation procedures to incorporate Red Team qualification, training, and certifications in the Certification decision as required by DoD Directive (DoDD) 8570.01, "Information Assurance Training, Certification, and Workforce Management," 23 April 2007.

(3) (U) Reaffirm following procedures for a quorum to be present before certifying Red Teams in accordance with the NSA, "Evaluator Handbook for Red Team Certification and Accreditation," 17 June 2010, and develop procedures for any deviations from the established procedures to be formally documented and approved.

(4) (U) DoD OIG Recommendation: Review and evaluate the 57th Information Aggressor Squadron (IAS) and the 177th IAS as separate Red Teams for Certification and Accreditation.

(5) (U) Review the validity of the Red Team Accreditation letter given to the 57th Adversary Tactics Group (ATG).

~~(S)~~ <sup>NSA; OSD/JS, STRATCOM (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g); NSA (b)(3)</sup>

(U) USSSTRATCOM Response to (3): The NSA Handbook is being replaced with Chairman of the Joint Chiefs of Staff Manual 6510.03, *Department of Defense (DoD) Cyber Red Team Certification and Accreditation (C&A)*. It includes the requirement that the Cyber Red Team evaluation teams consist of at least six members and that any deviations from the requirements of

~~SECRET//NOFORN~~

~~SECRET//REL USA, FVEY~~

the Manual must be coordinated through the Certification Authority and approved by the Accrediting Authority. This change is being made to provide an official DoD-level document for the C&A of DoD Cyber Red Teams.

(U) USSTRATCOM Response to (4) and (5): USSTRATCOM/USCYBERCOM will work with the NSA Red Team to schedule an onsite evaluation of the 177<sup>th</sup> IAS. USSTRATCOM will provide updated accreditation letters for the 57<sup>th</sup> ATG and 177<sup>th</sup> IAS, as appropriate, based on the outcome of the evaluations.

3. (U) Please direct any questions to our POC, [REDACTED],  
USCYBERCOM/34. COMM: [REDACTED], NIPR E-mail: [REDACTED] or SIPR  
E-mail: [REDACTED].

*Kerry E. Kelley*  
KERRY E. KELLEY  
SES, DAF  
Director, C4 Systems

~~SECRET//REL USA, FVEY~~



DEPARTMENT OF DEFENSE  
UNITED STATES STRATEGIC COMMAND

NOV 07 2012

Reply To:  
USSTRATCOM/J67  
901 SAC BLVD STE 2317  
OFFUTT AFB NE 68113 6600

MEMORANDUM FOR THE OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF  
DEFENSE

Subject: USSTRATCOM Response to DoD OIG Project No. D2011-D000LC-0242.000

1. References:

a. DoD OIG Project No. D2011-D000LC-0242.000, *Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness*, 28 September 2012.

b. USSTRATCOM Response to DoD OIG Project No. D2011-D000LC-0242.000, 6 November 2012.

2. USSTRATCOM agrees with the DoD OIG recommendations to the Commander, USSTRATCOM as identified in reference a, items A2 and C1a-e, and responded to in reference b.

3. Please direct any questions to my POC [REDACTED] USSTRATCOM/J674, COMM: [REDACTED]

CHARLES L. NICHOLSON  
GIS-15, DAFC  
Chief, Cybersecurity Assurance Division

~~SECRET//NOFORN~~

**National Security Agency/Central Security  
Service Comments**

**Final Report  
Reference**



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE**  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

31 October 2012

**MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR READINESS,  
OPERATIONS, AND SUPPORT**

**SUBJECT: DoD Audit of the Red Team (Project No. D2011-D000LC-0242.000) -  
INFORMATION MEMORANDUM**

Thank you for the opportunity to review and comment on the draft report "Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness." NSA/CSS has reviewed the recommendations for the NSA/CSS Red Team listed in the recommendations table and provides comments via the enclosed matrix.

NSA (b)(3), (b)(6)

**KEITH B. ALEXANDER**  
General, U.S. Army  
Director, NSA/Chief, CSS

Encl:  
a/s

Declassify upon removal of enclosure.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**(U) Comment Matrix**

**(U) 2012-10614 DoD Audit of the Red Team  
"Better Reporting and Certification Processes Can Improve Red Teams'  
Effectiveness**

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

1

Final Report  
Reference

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

#	Section w/ Page # Line #	Paragraph	POC:	NSA Red Team Comments	Report Recommendations
1.	Page 12	Para 3, A.3.	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]; NSA OGC/A&CS, [Redacted]	(U) Disagree; CJCSI 6510.01F Section B.8 delineates the responsibilities of the Director, NSA (DIRNSA)/Chief, CSS when NSA Red Team is providing support to DoD entities (e.g., providing an assessment of the DoD entities' systems at the request of those entities). This section does not direct DIRNSA to provide NSA Red Team reports to the specified distribution. Rather, the CJCSI (Section C.6(i)) directs the assessed entity to provide to the specified distribution any red team reports on the entity's system, which may include those generated by the NSA Red Team on behalf of the entity.  Currently, DIRNSA, as the head of a DoD Component, is responsible under the CJCSI for directly providing to the specified distribution only those NSA Red Team reports associated with NSA Red Team assessments of NSA systems. (Section C.6(i))  NSA recognizes that enabling it to directly provide to the specified distribution NSA Red Team reports of assessed DoD systems (when NSA has been requested to do those assessments on behalf of other DoD entities) would add rigor to the protection of DoD IS. However, currently there is no express direction in DoD regulations for DIRNSA to do this.	(U//FOUO) A.3. NSA (b)(3) [Redacted] NSA (b)(3) [Redacted]

Revised  
Recommendation A.3

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**Final Report  
Reference**

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

#	Section w/ Page # Line #	Paragraph	POC:	NSA Red Team Comments	Report Recommendations
				As such, NSA believes the recommendation should be recharacterized, as indicated in the next column.	
2.	Page 23-24	B.1	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]	(U) Agree; however, see recommended wording in this and next column. DoD Components may only develop such policy for the systems for which they have responsibility. Recommendation should be re-worded to clarify this. See recommended wording in next column.	(U//FOUO) B.1 We recommend that the NSA: (b)(3) [Redacted]
3.	Page 24	B.2	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]	(U) Agree; however, see suggested wording for clarification in the next column.	(U//FOUO) B.2 We recommend that the NSA: (b)(3) [Redacted]
4.	Page 29	Para 1, C.1.a.	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]	(U) Agree. Will work with U.S. Strategic Command in FY13 to address the issue and identify a way forward.	(U//FOUO) C.1. We recommend that the NSA: (b)(3) [Redacted]

Revised  
Recommendation B.1

Revised  
Recommendation B.2

Revised  
Recommendation C.1

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Final Report  
Reference

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

#	Section w/ Page # Line #	Paragraph	POC:	NSA Red Team Comments	Report Recommendations
					NSA: (b)(3)
5.	Page 29	Para 1, C.1.b.	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]	(U) Agree; however, this will take time to develop and deliver due to the unique skill sets of each Red Team and the current demand signal which stretches us beyond capacity.	(U//FOUO) b. NSA: (b)(3)
6.	Page 29	Para 1, C.1.c.	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]	(U) Agree. NSA Red Team will adhere to quorum requirement.	(U//FOUO) c. NSA: (b)(3)
7.	Page 29	Para 1, C.1.d.	(U//FOUO) [Redacted] Chief NSA Red Team, [Redacted]	(U) Agree. Will determine a new evaluation date once the Certification & Accreditation qualification for Red Teams is revised.	(U//FOUO) d. NSA: (b)(3)
8.	Page 29	Para 1, C.1.e.	(U//FOUO) [Redacted] Chief NSA [Redacted]	(U) Agree. The letter should be revised if needed, and written to the Element of the onsite evaluation.	(U//FOUO) e. NSA: (b)(3)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**Final Report  
Reference**

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

#	Section w/ Page # Line #	Paragraph	POC:	NSA Red Team Comments	Report Recommendations
			Red Team, [REDACTED]		

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

5

# U.S. Army Cyber Command/2nd Army Comments

Final Report  
Reference



REPLY TO  
ATTENTION OF:

ARCC-CG

6 NOV 12

DEPARTMENT OF THE ARMY  
UNITED STATES ARMY CYBER COMMAND/2<sup>ND</sup> ARMY  
8825 BEULAH STREET  
FT BELVOIR VA 22060-5248

MEMORANDUM FOR Department of Defense Inspector General (DoDIG), ATTN: Ms. [REDACTED] Project Manager, Readiness, Operations, and Support, 4800 Mark Center Drive, Alexandria, Virginia 22350-1500

SUBJECT: Command Reply to DoDIG Draft Report – “Better Reporting and Certification Processes Can Improve Red Teams’ Effectiveness” dated September 28 2012 (DoD IG Project No. D2011-D000LC-0242.000)

1. Thank you for the opportunity to comment on the subject report.
2. The U.S. Army Cyber Command/2<sup>nd</sup> Army (ARCYBHR) has reviewed the subject draft report and submits the attached response. With respect to Recommendations A.6a. and A.6b., this constitutes the official Army response.
3. My POC for this action is [REDACTED] Director, Office of Internal Review, [REDACTED]  
[REDACTED]

*Rhett A. Hernandez*  
RHETT A. HERNANDEZ  
Lieutenant General, US Army  
Commanding

DOD IG DRAFT REPORT DATED DATED SEPTEMBER 28 2012  
DOD IG PROJECT NO. D2011-D0001.C-0242.000

"BETTER REPORTING AND CERTIFICATION PROCESSES CAN  
IMPROVE RED TEAMS' EFFECTIVENESS"

ARMY CYBER COMMAND COMMENTS  
TO THE DOD IG RECOMMENDATIONS

~~(U//FOUO)~~ RECOMMENDATION A.6.a: DoD IG recommends that the Commander, 1st Information Operations Command develop procedures to validate that Red Teams distribute their reports to the U.S. Strategic Command, Defense Information Systems Agency, National Security Agency, Defense Threat Reduction Agency, and Director, Operational Test and Evaluation in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011.

(U) ARMY RESPONSE: Concur with comments.

(U) Comments: The Recommendations should have been directed to the Commander, US Army Cyber Command/2nd Army. Commander, US Army Cyber Command will implement the recommendation.

Redirected, and  
Renumbered  
Recommendation  
A.6.a to A.4.a

~~(U//FOUO)~~ RECOMMENDATION A.6.b: DoD IG recommends that the Commander, 1st Information Operations Command develop procedures to review agreements to determine if they contradict current DoD policies, standards, and regulations.

(U) ARMY RESPONSE: Concur with comments.

(U) Comments: The Recommendations should have been directed to the Commander, US Army Cyber Command/2nd Army. Commander, US Army Cyber Command will implement the recommendation.

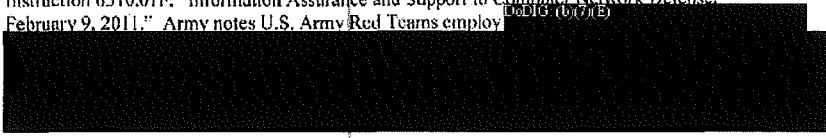
Redirected and  
Renumbered  
Recommendation  
A.6.b to A.4.b

(U) INTERNAL CONTROLS: DoD IG identified internal control weaknesses, specifically: "for vulnerability assessment reporting, NSA, Fleet Cyber Command and Navy 10<sup>th</sup> Fleet, the 57<sup>th</sup> ATG, and the 1<sup>st</sup> IO Command determined: it to be more efficient to produce a generic template of recommendations, some findings were not significant enough to report, and a briefing to the Chief Information Officer (CIO) was sufficient instead of a report. Also, they agreed to not release reports to DoD Components without approval of the assessed organization."

(U) ARMY RESPONSE: Army acknowledges the identified information.

(U) Comments: The internal control issues identified will be remedied through implementation of recommendations articulated in Recommendations A.6.a. and A.6.b.

(U//FOUO) FURTHER COMMENTS ON THE REPORT AS A WHOLE: Regarding Recommendation A.2.: "We recommend that the Commander, U.S. Strategic Command, develop a standard report format for Red Teams in accordance with the Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011." Army notes U.S. Army Red Teams employ <sup>(U//FOUO)</sup>





~~SECRET//NOFORN~~

# U.S. Fleet Cyber Command/U.S. Tenth Fleet Comments

Final Report  
Reference

~~FOR OFFICIAL USE ONLY (FOUO)~~



## DEPARTMENT OF THE NAVY

COMMANDER  
U.S. FLEET CYBER COMMAND  
9800 SAVAGE ROAD, SUITE 6586  
FORT GEORGE G. MEADE, MD 20765-6586

3200  
Ser N3/795  
13 Nov 12

From: Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet  
To: Department of Defense, Office of Inspector General

Subj: U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET (FCC/C10F)  
COMMENTS REGARDING DRAFT DOD IG REPORT, "BETTER REPORTING  
AND CERTIFICATION PROCESS CAN IMPROVE RED TEAMS'  
EFFECTIVENESS (PROJECT NO. D2011-D000LC-0242.000)

Ref: (a) DoD Draft IG Report of 28 Sep 12

1. The following responds to recommendations from the draft Department of Defense (DoD), Office of Inspector General (IG) report, reference (a): Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness (Project No. D2011-D00LC-0242.000) dated 28 September 2012.

a. U.S. Strategic Command (USSTRATCOM) should develop a standard reporting format that incorporates policies to ensure Red Teams report all findings, (pg i).

Concur with recommendation. Specific comments:

(1) If combined with DoD IG's recommendation about increased distribution of the reports (below), a standardized report format will allow different entities across DoD to understand key information from each service Red Teams' assessment, and better enable clear and consistent reporting.

(2) Caveat: Report format should allow each service to customize a portion due to unique configurations of assessed networks. Infrastructure and configurations for naval entities are vastly different than land based infrastructure/configurations.

b. ~~NSA (S//NF)~~

Concur with recommendation. Specific comments;

~~FOR OFFICIAL USE ONLY (FOUO)~~

~~SECRET//NOFORN~~

~~FOR OFFICIAL USE ONLY (FOUO)~~

Subj: U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET (FCC/C10F)  
COMMENTS REGARDING DRAFT DOD IG REPORT, "BETTER REPORTING  
AND CERTIFICATION PROCESS CAN IMPROVE RED TEAMS'  
EFFECTIVENESS (PROJECT NO. D2011-D000LC-0242.000)

(1) The current Certification and Accreditation (C&A) process is heavily focused on the administrative aspects of a Red Team, documenting qualifications, ensuring complete SOPs, infrastructure protection. The process needs to be expanded to include the capability to assess the service Red Team's operational proficiency and capability to meet mission. This should include periodic C&A team observations during Red Team operations.

c. A.4. We recommend that the Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet; Establish procedures to verify Red Team reports include recommendations that are specific to each identified finding, (pg 12)

Concur with recommendation, appropriate actions in progress.  
Specific comments:

(1) It was noted the Navy Red Team (NRT) final report did include some mitigation recommendations but did not address all discovered vulnerabilities. NRT has already changed its Final Reporting process to ensure ALL vulnerabilities that NRT discovers in an operation have a recommended mitigation.

(2) NRT's mitigation recommendations are based on an adversary's viewpoint. Recommendations are from neither a holistic nor complete cyber enterprise coordinated perspective.

(3) NRT is not tasked, structured nor resourced as a vulnerability mitigation organization. NRT's primary function is to create effects during exercises and operations. Vulnerability mitigation effort needs to be coordinated throughout the cyber enterprise (e.g. NCF, other TYCOMS, NCDOC, SPAWAR, and other SYSCOMs) with NRT positioned to provide recommendations for mitigation.

d. Develop procedures to validate that Red Teams distribute their reports to the USSTRATCOM, Defense Information Systems Agency, NSA, Defense Threat Reduction Agency, and Director, Operational Test and Evaluation (DTO&E) in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," 9 February 2011, (pg 12)

Renumbered  
Recommendation  
A.4.a to A.5.a

Renumbered  
Recommendation  
A.4.b to A.5.b

~~FOR OFFICIAL USE ONLY (FOUO)~~

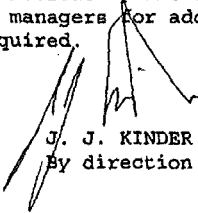
~~FOR OFFICIAL USE ONLY (FOUO)~~

Subj: U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET (FCC/C10F)  
COMMENTS REGARDING DRAFT DOD IG REPORT, "BETTER REPORTING  
AND CERTIFICATION PROCESS CAN IMPROVE RED TEAMS'  
EFFECTIVENESS (PROJECT NO. D2011-D000LC-0242.000)

Concur with recommendation to increase distribution for joint  
tasked Red Team activities via DTO&E as appropriate. For  
service tasked activities, distribution should be controlled at  
the service level. Specific comments:

(1) NRT does reports to the command requesting support  
(e.g. CSFTL, CSFTP, C3F, etc) and to FCC/C10F for assessments.

(2) FCC/C10F is the interface point with the HHQs,  
SYSCOMs, TYCOMs, and program managers for addressing identified  
issues as appropriate and required.

  
J. J. KINDER  
By direction

~~FOR OFFICIAL USE ONLY (FOUO)~~

3

# Joint Forces Headquarters Kansas Comments

Final Report  
Reference



DEPARTMENTS OF THE ARMY AND THE AIR FORCE  
JOINT FORCES HEADQUARTERS KANSAS  
2800 SOUTHWEST TOPEKA BOULEVARD  
TOPEKA, KS 66611-1287

NGKS-IMZ

05 November, 2012

MEMORANDUM FOR DoD Office of Inspector General

FROM: Kansas Chief Information Officer/Director of Information Technology


SUBJECT: Management Comments Re: DoD OIG Project Number D2011-D000LC-0242.000

1. In response to Recommendations B.1 and B.4 presented in the above referenced project, the Kansas JFHQ Directorate of Information Technology offers the following:

- A. Concur. Referenced Esker License Control Software supported legacy hardware that is no longer in use. Since the DoD OIG visit, all instances of this software have been removed as verified by network scans.
- B. Concur. Referenced SIPRNET-related documents no longer reside on the shared network drive. It should be noted that these documents were not classified and their presence violated no regulation. Their removal, however, is prudent in terms of overall risk management.
- C. Concur. State has migrated entire architecture from Cisco Level 7 to DoDIG (b)(7)(E) DoDIG (b)(7)(E)
- D. Non-concur. A goal of monitoring information posted on the internet by all employees of the organization is untenable. Due diligence is currently exercised through an agency-published social media Standard Operating Procedure. Public Web content is a Public Affairs function. The agency Public Affairs Office approves content for all official web pages and official social media sites. The PAO also subscribes to services that alert them when keywords concerning the Kansas National Guard are posted.
- E. Non-concur. Kansas systems exist as a tenant on the National Guard Bureau (NGB) domain. All internet traffic is routed through NGB routers and firewalls. NGB maintains a web cache that controls access to unauthorized sites. This recommendation is not a state-level issue.

2. The Directorate also feels obligated to mention that the purpose of this DoD OIG visit was not accurately presented to JFHQ Kansas prior to their arrival. The Directorate was led to believe that the DoD Red Teams were the focus and that the OIG was visiting Kansas to capture our level of satisfaction with the product we received and to help the OIG develop checklists for future *actual* evaluations. In addition, and in hindsight, the Red Team's JFHQ Kansas visit was not a suitable candidate for this OIG evaluation. This was not an assigned mission for the Red Team. It was an in-state, unit-to-unit request for a vulnerability "quick-look"; the structure, findings and recommendations were understood to be informal, completed on a time-available basis and to be shared between the Directorate and the Red Team Chief.

3. Questions may be addressed to the below.

  
CHRIS A. STRATMANN  
Col, NGKS  
Chief Information Officer/Director of Information Management

~~SECRET//NOFORN~~

# Biometrics Identity Management Agency Comments

Final Report  
Reference

~~SECRET//NOFORN~~



REPLY TO  
ATTENTION OF  
DAPM-ZB

NOV 5 2012

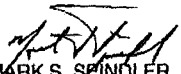
DEPARTMENT OF THE ARMY  
OFFICE OF THE PROVOST MARSHAL GENERAL  
2800 ARMY PENTAGON  
WASHINGTON DC 20310-2800

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL, 4800  
MARK CENTER DRIVE, ALEXANDRIA, VA 22350-1500

SUBJECT: DODIG Draft Audit Report - Better Reporting and Certification Processes Can  
Improve Red Teams' Effectiveness (11LC-0242)

1. Reference Department of Defense Inspector General (DoDIG) Report 11LC-0242,  
28 Sep 12, SAB.
2. Thank you for the opportunity to review and respond to subject draft report. The  
Office of the Provost Marshal General, Biometrics Identity Management Agency (BIMA)  
concur with the report with exception to paragraph 2, page 23. Responses to the  
recommendations addressed to BIMA in addition to comments on internal control  
weaknesses are enclosed.
3. My point of contact is [REDACTED]

Encl  
as

  
MARK S. SPINDLER  
Colonel, MP  
Deputy Provost Marshal General

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

**Final Report  
Reference**

~~SECRET//NOFORN~~

**DODIG Draft Report  
Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness  
(11LC-0242)**

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

**DODIG Draft Report  
Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness  
(11LC-0242)**

OSD/JS: (b)(1), Sec. 1.4(a), 1.4(e), 1.4(g)



~~SECRET//NOFORN~~

Page 28

Revised page 27

# Program Executive Office, Enterprise Information Systems Comments

Final Report  
Reference



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
OFFICE OF THE PROGRAM EXECUTIVE OFFICER  
ENTERPRISE INFORMATION SYSTEMS  
(PEO EIS)  
8350 HALL ROAD  
FORT BELVOIR, VIRGINIA 22060-6526


NOV 13 2012

SFAE-PS

MEMORANDUM FOR Inspector General, Department of Defense, 4800 Mark Center Drive,  
Alexandria, Virginia 22350-1500

SUBJECT: Security Review of Draft Audit Report, "Better Reporting and Certification  
Processes Can Improve Red Teams' Effectiveness," Project No. D2011-D0001.C-0242.000 dated  
September 28, 2012.

1. Per the request dated September 28, 2012, PEO EIS and PM Biometrics have reviewed the Draft Audit Report, prepared a Plan of Action and Milestones (POA&M) per paragraph B.6 and submitted to requesting office via SIPRNet November 2, 2012 filename (U//S)DoD ABIS PenTest POAM(SECRET)Final.xlsx". In accordance with paragraph B.1, PEO EIS has a Certification and Accreditation Policy in place for reporting and resolving security weaknesses utilizing the POA&M process. Also, to ensure that this does not occur in the future, PEO EIS Information Assurance Program Manager (IAPM) is now on distribution lists from the Regional Computer Emergency Response Team CONUS for all persistent security tests and has been negotiating future Red/Blue Team assessments for PEO EIS systems.
2. The POA&M was classified in accordance with the draft report portion markings and no other comments were made on the contents of the report.
3. My point of contact for this action is [REDACTED] PEO EIS IAPM, [REDACTED] email:  
[REDACTED]

  
TERRY J. WATSON  
Deputy PEO EIS

~~FOR OFFICIAL USE ONLY~~



**Final Report  
Reference**

OSDJS: (b)(1), Sec. 1.4(a), 1.4(c), 1.4(g)



~~SECRET~~  
D O I  
Classified By: 50,515 JAFM  
Declassify On: OADR, Report # EAO 2001-02000, CAC 02-000, EAO 21 Sep 2012  
Declassify On: ~~SECRET~~

# 57th Adversary Tactics Group (ACC) Comments

Final Report  
Reference



DEPARTMENT OF THE AIR FORCE  
57TH ADVERSARY TACTICS GROUP (ACC)  
NELLIS AIR FORCE BASE, NEVADA

21 October 2012

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL  
ATTN: [REDACTED] Project Manager, Readiness, Operations, and Support  
FROM: 57 ATG/CC  
SUBJECT: 57 ATG/CC Response to DOD IG Report (Project No. D2011-D0001C-0242.000)

1. As a recap of your audit, the 4 action areas for 57 ATG were:
  - a. Establish procedures verifying Red Team reports include all identified findings.
  - b. Establish procedures verifying Red Teams create reports for all missions.
  - c. Develop procedures validating Red Team report distribution IAW CJCSI 6510.01F.
  - d. Develop procedures to identify contradictions in Red Team SOPs and DOD guidance.
2. Answers/responses:
  - a. We agree debriefing operators on deviations from specific desired learning objectives is vital to improvement. Aggressors provide feedback in many ways: after action reports, technical debriefs, verbal debriefs, and lessons learned.
  - b. We are modifying Information Aggressor operating standards and will include new verbiage on the requirement to report mission findings in accordance with USSTRATCOM procedures. Expect this in ATGI 10-2-IAS Volume 3 – Information Aggressor Operations Standards.
  - c. We are developing cross-check procedures to continually identify contradictions between Red Team SOPs and DOD guidance. Expect this in ATGI 10-2-IAS Volume 3 – Information Aggressor Operations Standards.
3. Training versus Inspections. The Air Force “Red Team” mission has grown over time. Our Information Aggressor squadrons integrate with aggressors in the air, surface-to-air, and space domains creating an integrated, contested environment for training blue forces. It is important for aggressors not be viewed as “inspectors.” There are times that non-attribution may be agreed upon for training to ensure we present a realistic exercise environment to maximize training effects and debrief focus points. Training events are vital to readiness, learning and improvement apart from the formal inspection process. Similarly, there are other times when aggressors provide forces for IG teams to validate readiness posture. These events are coordinated with MAJCOM/IGs and reports are produced and disseminated through IG channels.
4. Aggressors conduct the best possible debriefs making blue forces better. We will continue providing feedback in the appropriate format as events or missions dictate.
5. Please direct any questions to my action officer, [REDACTED] 57 IAS/DO, at [REDACTED]

PETER S. FORD, Col, USAF  
Commander

Renumbered  
Recommendations  
A.5.a, A.5.b, A.5.c, and  
A.5.d to A.6.a, A.6.b,  
A.6.c, and A.6.d  
respectively

Response 2.a  
corresponds with  
Recommendation  
A.6.b

Response 2.b  
corresponds with  
Recommendations  
A.6.a and A.6.c

Response 2.c  
corresponds with  
Recommendation  
A.6.d

(U) **Annex. Sources**

~~(FOUO)~~ Source 1: Chairman of the Joint Chiefs of Staff Execute Order to Incorporate Realistic Cyberspace Conditions into Major DoD Exercises (Document classified ~~SECRET//RELTO USA, FVEY~~)

Declassify On: 20360201  
Date of Source: February 11, 2011

~~(FOUO)~~ Source 2: 57<sup>th</sup> Adversary Tactics Group Mobile Training Team Final Report, Kirtland Air Force Base (Document classified ~~SECRET//NOFORN//MR~~)

Declassify On: 20360707  
Date of Source: 7 Jul 2011

~~(FOUO)~~ Source 3: 57<sup>th</sup> Adversary Tactics Group Joint Forces Headquarters Briefing (Document classified ~~SECRET~~)

Declassify On: 20370107  
Date of Source: 7 Jan 2012

~~(FOUO)~~ Source 4: Cyber Defense Assessment Team Activity Report for USS George H.W. Bush Strike Group Joint Task Force Exercise 11-4 (Document classified ~~SECRET//NOFORN~~)

Declassify On: 20360317  
Date of Source: 17 Mar 2011

~~(FOUO)~~ Source 5: Cyber Defense Assessment Team Activity Report for USS Enterprise Strike Group Joint Task Force Exercise 11-2 (Document classified ~~SECRET//NOFORN~~)

Declassify On: 20360106  
Date of Source: 6 Jan 2011

~~(FOUO)~~ Source 6: Biometrics Identity Management Agency and Automated Biometric Information System Red Vulnerability Assessment Report (Document classified ~~SECRET//NOFORN~~)

Declassify On: 20351025  
Date of Source: 28 Nov 2010

~~(FOUO)~~ Source 7: <sup>NSA (b)(3)</sup> 

<sup>NSA (b)(3)</sup> 

~~SECRET//NOFORN~~

(FOUO) Source 8: <sup>NSA: (b)(3)</sup>



Declassify On: 20360523  
Date of Source: 23 May 2011

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



Inspector General  
Department of Defense

~~SECRET//NOFORN~~