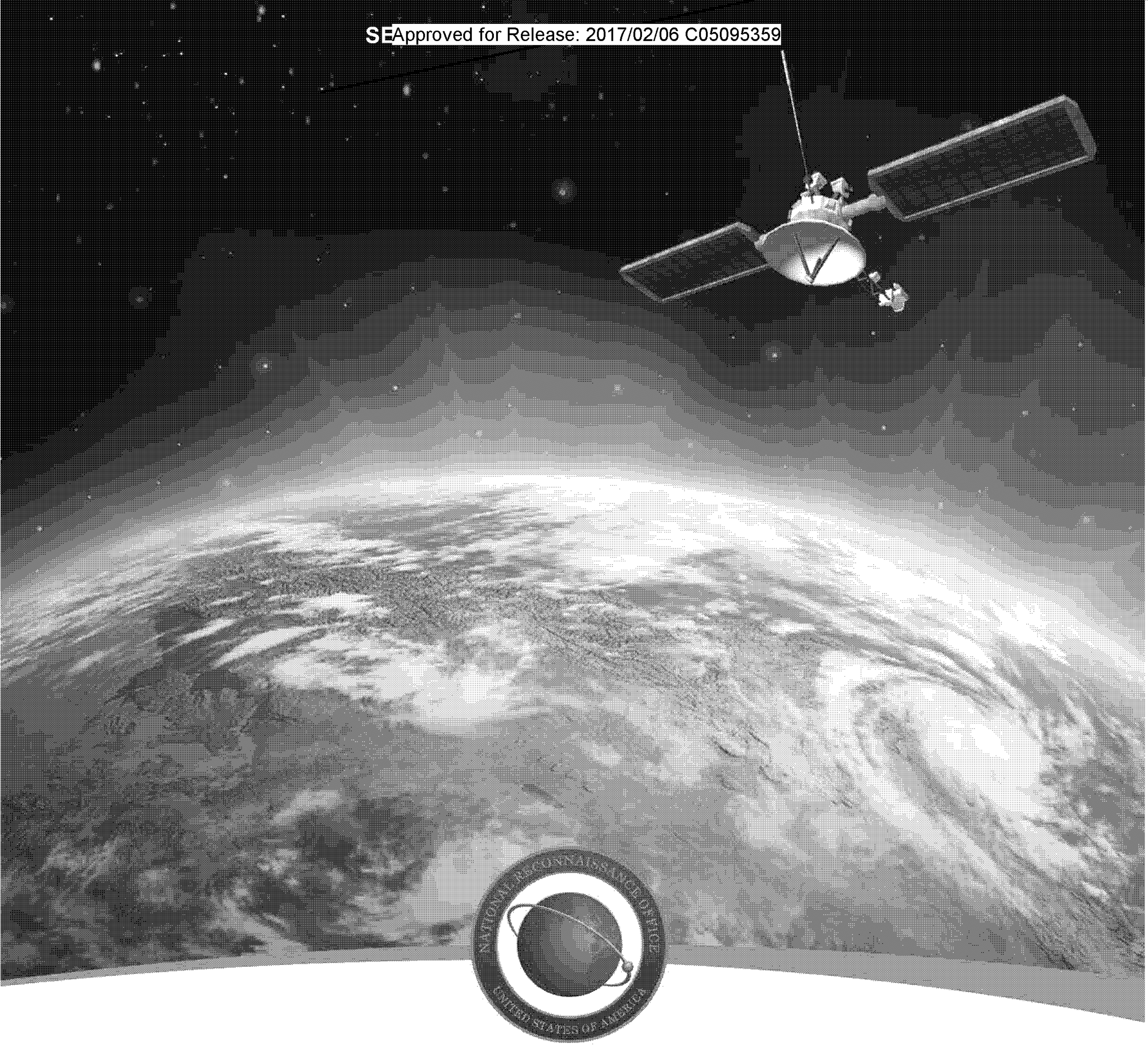


NATIONAL RECONNAISSANCE OFFICE

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

(U) Audit of NRO Cyber Incident Detection and Response

(Project Number 2014-001 A)

(b)(3)

17 December 2014

CL BY:
DECL ON: 20391217
DRV FM: INCG 1.0, 13 February 2012

This document cannot be released in whole or in part to persons or agencies outside the NRO, nor can it be republished in whole or in part within any document not containing this statement, without the express written approval of the NRO Inspector General.

~~SECRET//TALENT KEYHOLE//NOFORN~~

THIS PAGE INTENTIONALLY LEFT BLANK

Unless noted, redactions on this page fall under Exemption (b)(3).

NATIONAL RECONNAISSANCE OFFICE

Office of Inspector General
14675 Lee Road
Chantilly, VA 20151-1715

17 December 2014

MEMORANDUM FOR DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
PRINCIPAL DEPUTY DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DEPUTY DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTOR, COMMUNICATIONS SYSTEMS DIRECTORATE/ CHIEF INFORMATION OFFICER
DIRECTOR, OFFICE OF SECURITY AND COUNTERINTELLIGENCE

SUBJECT: (U) Final Report: Audit of the National Reconnaissance Office Cyber Incident Detection and Response (Project Number 2014-001 A)

(U//~~FOUO~~) The National Reconnaissance Office (NRO) Office of Inspector General (OIG) report on the *Audit of NRO Cyber Incident Detection and Response* is attached. I am providing this report for the Communications Systems Directorate's (COMM's) and Office of Security and Counterintelligence's (OS&CI's) information and implementation of the recommendations. In implementing your proposed plans to address and resolve each recommendation, COMM and OS&CI are required to report via the TIER system on the status of actions taken and estimated completion dates.

(U//~~FOUO~~) I appreciate the courtesies extended to my staff during this audit. Please direct any questions you may have regarding this report to [redacted] Auditor-in-Charge, at [redacted] (secure), or [redacted] Deputy Assistant Inspector General, at [redacted] (secure). Please direct any questions you may have regarding corrective action reporting to [redacted] OIG Follow-up Administrator, at [redacted]

Adam G. Harris
Inspector General

Attachment:
(U) Final Audit Report
(Project Number 2014-002 A) ~~(S//TK//NF)~~

CL BY: [redacted]
DECL ON: 20391217
DRV FROM: INCG 1.0, 13 February 2012

UNCLASSIFIED//~~FOUO~~ when separated from document

THIS PAGE INTENTIONALLY LEFT BLANK

Unless noted, redactions on this page fall under Exemption (b)(3).

SUBJECT: (U) Final Report: Audit of the National Reconnaissance Office Cyber Incident Detection and Response (Project Number 2014-001 A)

[redacted]/17 Dec 14

DISTRIBUTION:

Hard copy:
Director, National Reconnaissance Office
Principal Deputy Director, National Reconnaissance Office
Deputy Director, National Reconnaissance Office
Director, Communications Systems Directorate/Chief Information Officer
Director, Office of Security and Counterintelligence
Deputy Assistant Inspector General, [redacted]
Auditor-in-Charge, [redacted] (for official file)
Follow-up Administrator, [redacted]
OIG Library
Chron

Soft copy:
IG-Followup-Tracker (TIER)
OIG External Webpage
NROnet

THIS PAGE INTENTIONALLY LEFT BLANK

Unless noted, redactions on this page fall under Exemption (b)(3).

EXECUTIVE SUMMARY

(U) Audit of NRO Cyber Incident Detection and Response

(U) To view the full report, including the scope, methodology, results, and management comments, go to https://corpstaff.svc.nro.ic.gov/oig

(U) Why the OIG Did This Audit

(~~S//NF~~) Successful penetration or disruption of [redacted] NRO classified networks are high priority targets for our adversaries [redacted] (b)(1) (b)(3) As an incentive for the NRO to improve cyber incident detection and response capabilities, the Fiscal Year 2014 Intelligence Authorization Act fenced [redacted] from the NRO's budget and directed the NRO to develop a strategy and implementation plan that addresses the [redacted] S//NF

(U//~~FOUO~~) The OIG conducted this audit to determine the NRO's effectiveness in preventing, detecting, and responding to cyber incidents. Specifically, the OIG assessed whether the NRO has adequate controls in place to ensure cyber incidents on NRO networks and systems are detected and handled in accordance with applicable laws and regulations.

(b)(1)
(b)(3)

(U) What the OIG Found

S//NF

(U//~~FOUO~~) Overall, the NRO's effectiveness in preventing, detecting, and responding to cyber incidents [redacted]

(~~S//NF~~) [redacted] (b)(1) (b)(3)

[redacted] (b)(1) (b)(3)

(U//~~FOUO~~) The OIG also found that the NRO [redacted]

(U) What the OIG Recommends

(U//~~FOUO~~) The OIG recommends the NRO take [redacted] (b)(1) (b)(3) complete list of recommendations can be found Appendix A.

(U) Management Comments

(U) The Director, Communications Directorate (D, COMM) and Director, Office of Security and Counterintelligence (D, OS&CI) reviewed a draft of this report and concurred with the findings and recommendations presented. The D, COMM and D, OS&CI comments and plans meet the intent of the recommendations. As part of our follow-up process, we will monitor the status of the corrective action plans through full implementation. Complete copies of management comments can be found in Appendix F.

THIS PAGE INTENTIONALLY LEFT BLANK

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) OFFICE OF INSPECTOR GENERAL

(U) Audit of the National Reconnaissance Office Cyber Incident Detection and Response (Project Number 2014-001 A)

(U) INTRODUCTION

~~(S//NF)~~ National Reconnaissance Office (NRO) [redacted] (b)(1) (b)(3)

~~(S//NF)~~ Prior NRO network security assessments have shown [redacted] (b)(1) (b)(3) the 2012 NRO Office of Inspector General (OIG) *Audit of the NRO Enterprise Management of Cyber Incidents* identified that the NRO [redacted] the NRO's cyber incident detection and response capabilities, the fiscal year (b)(1) (FY) 2014 Intelligence Authorization Act fenced [redacted] from the NRO's budget and directs (b)(3) the NRO to develop a strategy and implementation plan that addresses the [redacted] (3) reporting of cyber incidents to Intelligence Community Security Coordination Center (IC SCC).

~~(U//FOUO)~~ The OIG conducted this audit to determine the NRO's effectiveness in preventing, detecting, and responding to cyber incidents. Federal guidance[1] defines a cyber incident as any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or information system without lawful authority. The OIG also assessed whether the NRO has adequate controls in place to ensure cyber incidents on NRO networks and systems are detected and handled in accordance with applicable laws and regulations.

(U) BACKGROUND

(U) The Federal Information Security Management Act (FISMA) of 2002 sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources supporting federal operations and assets. With regard to cyber incident detection and response, FISMA requires each agency to implement an information security program that includes procedures for detecting, reporting, and responding to cyber incidents. Further, NSPD - 54/HSPD - 23 requires federal agencies to (1) increase efforts to coordinate and enhance the security of classified and unclassified networks; (2) increase the protection of the data on these networks; and (3) improve their capability to deter, detect, prevent, protect against, and

[1] (U) National Security Presidential Directive (NSPD) – 54/Homeland Security Presidential Directive (HSPD) – 23

respond to threats against information systems and data. Appendix B provides a listing of policies and procedures applicable to NRO cyber incident detection and response functions.

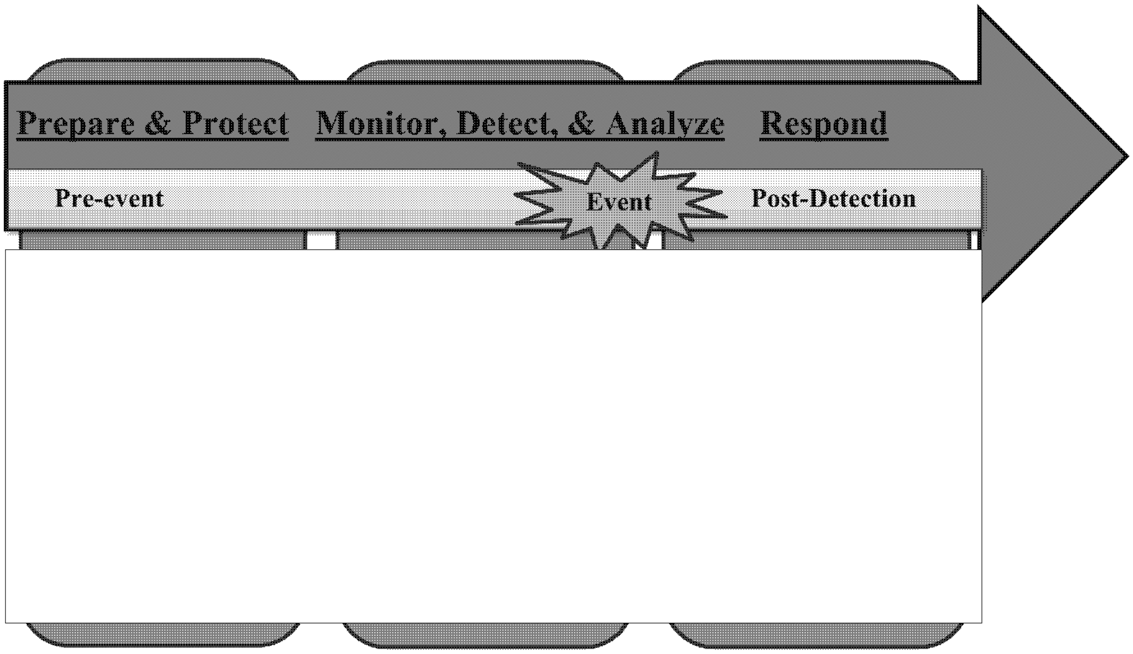
(U) Elements of Computer Network Defense

(U) Computer Network Defense (CND) operations include actions taken to (1) prepare and protect; (2) monitor, detect, and analyze; and (3) respond to unauthorized activity within information systems and networks. Figure 1 below shows the CND elements.

(U) Prepare and protect operations are the continuous day-to-day practices, capabilities, and procedures to manage the security of networks and systems. The preparation and protection phase also includes [redacted]

(U) Monitoring and detecting cyber incidents is a continuous process of identifying any unusual network or system activity that has the potential to adversely affect systems, networks, or operational missions. Monitoring and detection also provides situational awareness, attack sensing, and indications and warnings. The primary objectives for detecting cyber incidents are to ensure that all suspicious activity is identified and reported in a timely manner consistent with required reporting timelines to facilitate further analysis and ensure effective coordination with other organizations.

(U) Once a cyber incident is detected, the ability to proactively respond to the unauthorized activity and events that might negatively impact the mission includes steps to prevent further damage, restore the integrity of affected systems, and implement follow-up strategies to prevent the incident from happening again.



[redacted]

(U) Figure 1: Computer Network Defense Elements

Figure is UNCLASSIFIED//~~FOUO~~

(U) NRO Cyber Incident Detection and Response

(U//~~FOUO~~) The NRO Chief Information Officer (CIO) establishes the cyber incident detection and response policy. The CIO is also responsible for providing oversight of cyber incident handling and reporting to external entities. However, the CIO does not have a role in the execution of these activities. Execution of these activities is performed by the Communications Systems Directorate (COMM), [redacted] is responsible for all NRO information technology (IT) infrastructure and commoditized services to include incident detection and response, compute, storage, networks, and enabling commercial software.

(U//~~FOUO~~) The [redacted] was established in April 2014 to serve as the single NRO office responsible for providing unified, comprehensive cyber defense services for the NRO Information Enterprise (NIE).[3] Prior to the establishment of the [redacted] the [redacted] was responsible for the overall cyber incident detection and response function. With the implementation of the [redacted], all of [redacted]s resources for cyber defense and response transitioned to the [redacted] Currently, the [redacted] is chartered with 24 hours, 7 days a week monitoring of the NIE. As such, they are responsible for protecting, detecting, and responding to suspicious and unauthorized activity on or against the NIE. The [redacted] is also chartered to conduct scans of NRO networks, perform external security incident reporting with guidance from the [redacted] and maintain the NRO [redacted] Although the results of audit testing refer t[redacted]as the organization responsible for performing cyber incident detection and response, with its standup, the [redacted]nherited these responsibilities. As a result, the [redacted] responsible for performing cyber incident detection and response in the future.

(U//~~FOUO~~) The Office of Security and Counterintelligence (OS&CI) also supports the NRO's cyber incident and response efforts [redacted]

[2] (U//~~FOUO~~) Effective 15 September 2014, the Chief Information Office and Communications Systems Directorate (COMM) merged. With this merger, the Director, COMM assumed the Chief Information Officer designation.

[3] (U//~~FOUO~~) The NIE is defined as the collection of all NRO-owned information and IT required to perform the NRO mission. [redacted]

[4] (U) [redacted]

(U) SCOPE AND METHODOLOGY

(U) The OIG conducted this performance audit from January 2014 to September 2014 in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions. The OIG assessed the internal controls deemed significant within the context of the audit objectives. The OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

(U//~~FOUO~~) The OIG reviewed relevant laws and regulations, as well as Department of Defense (DoD), Office of Director of National Intelligence (ODNI), and NRO guidance, policies, and procedures. The OIG interviewed NRO personnel from CIO, COMM, OS&CI, and mission ground stations to understand their role in the NRO incident detection and response process. The OIG also met with personnel from the IC SCC and U.S. Cyber Command (USCYBERCOM) to understand their requirements and expectations for NRO cyber incident reporting. Additionally, the OIG met with personnel responsible for incident detection and response [redacted] to obtain an understanding of their operations and identified best practices. Since the [redacted] inherited [redacted] cyber incident detection and response responsibilities in April 2014, the OIG met wit[redacted] personnel to discuss preliminary findings and recommendations and their plans to improve the CND security landscape.

(U//~~FOUO~~) To determine whether the NRO had adequate controls in place to prevent and detect cyber incidents, the OIG interviewed officials from the CIO and COMM to determine the NRO's processes and procedures for [redacted]. The OIG compared the lists of networks provided by COMM and CIO to determine how consistently this information is tracked between the Directorates and Offices (Ds and Os). Further, the OIG obtained a list of [redacted] to determine whether monitoring capabilities in place maintain visibility into all NRO networks. The OIG also reviewed the [redacted] to determine whether the NRO maintains adequate controls to prevent and detect cyber incidents.

(U//~~FOUO~~) In addition, the OIG reviewed the results of prior CIO network security assessments and [redacted] reports for cyber incidents detected. The OIG reviewed these reports to identify [redacted] Further, the OIG interviewed representatives from the CIO and individual Ds and Os to obtain an understanding of the NRO's [redacted]

(U//~~FOUO~~) To determine the effectiveness of the NRO's response to cyber incidents, the OIG obtained a list of all cyber incident cases created by [redacted] during calendar year (CY) 2013. From this list, the OIG selected a judgmental sample to determine the extent to which the NRO is reporting cyber incidents to IC SCC and USCYBERCOM. Although the findings of a judgmental sample cannot be projected, we believe that our sample provides a sufficient basis for

Unless noted, redactions on this page fall under Exemption (b)(3).

our audit findings and conclusions. The OIG also assessed the completeness and validity of the incident case data. Any information system data used by the auditors or included in this report for informational purposes was not audited.

(U) PRIOR COVERAGE

(U/~~/FOUO~~) ~~In~~ the *NRO FY 2014 FISMA Evaluation Report*, dated 5 September 2014, the OIG noted that the NRO [redacted] and reporting process. This issue has been reported since the FY 2009.

(S~~//NF~~) In the *Audit of the Enterprise Management of Cyber Incidents*, dated 15 June 2012, the OIG found that the NRO [redacted]

(b)(1)
(b)(3)

(U) AUDIT RESULTS

~~(S//NF)~~ The NRO cyber incident detection and response capability is [redacted]

(b)(1)
(b)(3)

[redacted]

(b)(1)
(b)(3)

~~(U//FOUO)~~ Finding 1: The NRO [redacted] [redacted]

~~(S//NF)~~ The NRO [redacted]

(b)(1)
(b)(3)

(U) Network Mapping

~~S//NF~~

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

(b)(1)
(b)(3)

[5] (U) Transport networks provide reliable communication sessions between computers.

Unless noted, redactions on this page fall under Exemption (b)(3).

(~~S//NF~~) In December 2013, the OIG issued the *Audit of CIO Management of NRO Information Technology*, [redacted] (b)(1) (b)(3)

(~~S//NF~~) [redacted] (b)(1) (b)(3)

(~~S//NF~~) [redacted] during this audit, the OIG found it necessary to request a list of NRO networks from the CIO, COMM [redacted] and COMM [redacted] to determine the extent of the NRO awareness of its universe of networks. [redacted] (b)(1) (b)(3) Corporate Business Process Instruction (CBPI) 50-2E, *Enterprise Defense-Cyber Incident Response*, provides the NRO a uniform definition of "network". It defines a network as a "collection of interconnected components, based on a coherent security architecture and design. This may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices."

(~~S//NF~~) The OIG [redacted] (b)(1) (b)(3) COMM [redacted] The [redacted] As illustrated in Figure 2, [redacted] of the reported [redacted] Appendix C provides [redacted] the networks reported by the CIO and COMM.

(b)(1)
(b)(3)

[6] (~~S//NF~~) [redacted]

[7] (U) [redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

[redacted] (b)(1) (b)(3)

(U) Figure 2: Common Networks Reported by COMM and CIO
Figure is ~~SECRET//TK//NOFORN~~

(~~S//NF~~) [redacted] new information to the NRO. In October 2005, [redacted] [redacted] assessment identified [redacted] Subsequently, in CY 2007, the CIO [redacted] According to a CIO official, [redacted] (b)(1) (b)(3)

(~~S//NF~~) [redacted] (b)(1) (b)(3)

(U) Recommendation #1 for the Director, COMM:

[redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

(U//~~FOUO~~) Management Response: The Director, COMM concurred with this recommendation. The Director, COMM [redacted] A complete copy of the management comments is included in Appendix F.

(U) Cyber Threat Assessments

(~~S//NF~~) [redacted] Cyber threat assessments are intended to provide a basis for improved risk management and strategic information assurance (IA) planning that consider both threats and vulnerabilities. [redacted]

(b)(1)
(b)(3)

(U) Although it is the owner of Information Technology-Information Assurance-Information Management (IT-IA-IM), the CIO [redacted] IC Standard (ICS) 502-01, *IC Computer Incident Response and Computer Network Defense*, requires IC elements to conduct annual cyber threat assessments to identify and evaluate cyber threats to enterprise information systems, networks, and shared IC resources. Further, ICD 502 Concept of Operations (CONOPS) [redacted]

(~~S//NF~~) [redacted]

(b)(1)
(b)(3)

(~~S//NF~~) In addition to CIO cyber threat assessment efforts, [redacted] personnel stated that [redacted]

(b)(1)
(b)(3)

[redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

(b)(1)
(b)(3)

[redacted]

(U) Recommendation #2 for the Director, COMM:

[redacted]

(U//~~FOUO~~) Management Response: The Director, COMM concurred with this recommendation. A complete copy of the management comments is included in Appendix F.

(U) Vulnerability Scanning

(~~S//NF~~) [redacted] CBPI 50-2E, *Enterprise Defense – Cyber Incident Response,* [redacted]

(b)(1)
(b)(3)

(U) [redacted]

(~~S//NF~~) Although CBPI 50-2E identifies [redacted] as the organization responsible for [redacted]

(b)(1)
(b)(3)

1. (U) [redacted]
2. (U)
3. (U)
4. (U)
5. (U)
6. (U)

(b)(1)
(b)(3)

(U//~~FOUO~~) [redacted] historically, mission system owners have expressed concern over [redacted] the mission. In addition, [redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

[redacted]

(U) Mission Ground Stations

~~(S//NF)~~ [redacted] (b)(1) (b)(3)

(U) Table 1: Vulnerability Scanned Systems at ADE-C and ADE-E

[redacted] (b)(1) (b)(3)

Table is ~~S//NF~~

~~(U//FOUO)~~ The OIG discussed vulnerability scanning with [redacted] personnel and they [redacted]

(U) Recommendation #3 for the Director, COMM:

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

~~(U//FOUO)~~ Management Response: The Director, COMM concurred with this recommendation. A complete copy of the management comments is included in Appendix F.

(U) Network Security Assessments

(~~S//NF~~) The NRO [redacted] (b)(1) (b)(3)

(~~U//FOUO~~) In January 2014, the CIO, [redacted] established a framework, [redacted]

(U) Red Team

(~~S//NF~~) The NRO Red Team [redacted] (b)(1) (b)(3)

(~~S//NF~~) [redacted] (b)(1) (b)(3)

(U) Blue Team

(~~S//NF~~) The NRO Blue Team, [redacted] (b)(1) (b)(3)

[9] (~~U//FOUO~~) Red Team is a group of individuals authorized and organized to [redacted]

[10] (~~U//FOUO~~) Blue Team is responsible [redacted] (i.e., the Red Team). [redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

[redacted] supporting Business Plans and Operations (BPO) in June 2013; however, [redacted] engineering efforts. (b)(1) (b)(3)

(U//~~FOUO~~) REBL activities [redacted]

(U) Recommendation #4 for the Director, COMM:

[redacted]

(U//~~FOUO~~) Management Response: The Director, COMM concurred with this recommendation. A complete copy of the management comments is included in Appendix F.

(U) Recommendation #5 for the Director, OS&CI:

[redacted]

(U//~~FOUQ~~) Management Response: The Director, OS&CI concurred with this finding and recommendation. OS&CI is currently [redacted] effort. A complete copy of the management comments is included in Appendix F.

(U) Network Monitoring Strategy

(~~S//NF~~) The NRO [redacted] (b)(1) (b)(3)

Unless noted, redactions on this page fall under Exemption (b)(3).

(S//TK//NF) [redacted] (b)(1) (b)(3)

(S//NF) [redacted] (b)(1) (b)(3) (b)(5)

(U//FOUO) While the OIG [redacted] the NRO must ensure that institutional knowledge is documented and shared amongst key stakeholders (e.g., COMM and CIO leadership). [redacted] leadership acknowledged that [redacted] A senior [redacted] official stated that [redacted] (b)(3) (b)(5)

(U) Recommendation #6 for the Director, COMM:

(U//FOUO) [redacted]

(U//FOUO) Management Response: The Director, COMM concurred with this recommendation. A complete copy of the management comments is included in Appendix F.

(b)(1)
(b)(3)

Page Denied

(b)(1)
(b)(3)

Unless noted, redactions on this page fall under Exemption (b)(3).

Page Denied

(b)(1)
(b)(3)

Unless noted, redactions on this page fall under Exemption (b)(3).

Page Denied

Unless noted, redactions on this page fall under Exemption (b)(3).

[redacted]

(b)(1)
(b)(3)

[redacted]

(U) Figure 5: [redacted] Assessment Results Briefing Dates

Figure is UNCLASSIFIED//FOUO

(U//FOUO) ICS 502-01 requires IC elements to report vulnerability assessment information, status, and results to the agency's leadership. ICS 502-01 also requires IC elements to develop and maintain internal processes for elevating report on information system weaknesses, deficiencies, and/or vulnerabilities associated with reported incidents to the IC element senior leadership and stakeholders. Further, the ICD 502 CONOPS [redacted]

(U//FOUO) From 2008 to 2009 [redacted]

(b)(1)
(b)(3)

(b)(1)
(b)(3)

Page Denied

Unless noted, redactions on this page fall under Exemption (b)(3).

[redacted] (b)(1) (b)(3)

(U) Acquisition Center of Excellence, Acquisition Resource Center Unclassified Webserver

~~(S//NF)~~ [redacted] the Acquisition Center of Excellence, Acquisition Resource Center (ARC) unclassified webserver [redacted] (b)(1) (b)(3)

~~(S//NF)~~ While NRO Directive 52-15, *Risk and Vulnerability Assessments, Reviews and Updates*, defines basic responsibilities [redacted] [redacted] (b)(1) (b)(3)

(U) Recommendation #9 for the Director, COMM:

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

~~(U//FOUO)~~ Management Response: The Director, COMM concurred with this recommendation. A complete copy of the management comments is included in Appendix F.

(b)(3)
(b)(1)

[18] ~~(S//NF)~~ In April 2014, the CIO issued Policy Note 2014-03 providing guidance on the proper classification of IT vulnerabilities. [redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

(U//~~FOUO~~) Finding 3: NRO Cyber Incidents [redacted]

(U//~~FOUO~~) The NRO [redacted]

(U//~~FOUO~~) The IC SCC requires initial cyber incident reports be provided [redacted] of the incident occurrence. USCYBERCOM requires initial cyber incident reports be provided within a range of [redacted] depending on the incident category. The OIG reviewed all [redacted] cyber incident reports the NRO reported to the IC SCC and USCYBERCOM from January 2013 through February 2014. [redacted]

(U//~~FOUO~~) [redacted] According to the ODNI *Intelligence Community Incident Reporting Procedures*, IC agencies should report category 1-8 cyber incidents and events on its TOP SECRET networks to the IC SCC.[21] [redacted]

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

[19] (U) The IC SCC is the IC CIO's executive agent to monitor and oversee the integrated defense of the IC information environment. The NRO is required to report cyber incident information associated with its TOP SECRET systems and networks to IC SCC.

[20] (U) The USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of DoD information networks. The NRO is required to report cyber incident information associated with its systems and networks at the SECRET and below classification levels to USCYBERCOM.

[21] (U//FOUO) The IC SCC also requires reporting for any network that is funded through the National Intelligence Program.

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

Unless noted, redactions on this page fall under Exemption (b)(3).

[redacted]

(b)(1)
(b)(3)

Table is S//NF

(U//FOUO) [redacted] CBPI 50-2E establishes cyber incident-related responsibilities for the CIO, to include (1) providing oversight for the overall cyber-related incident handling and reporting process, and (2) providing guidance regarding external reporting of cyber-related incidents. Such CIO oversight would minimize inconsistent and untimely information in the reports provided to IC SCC and USCYBERCOM.

(U//FOUO) The reporting and subsequent sharing of cyber incidents among the IC elements directly supports the building of trust and cooperation across the IC elements. [redacted]

[redacted]

[23] (U) Appendix D provides a description of each cyber incident category.

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) Recommendation #10 for the Director, COMM:

[redacted]

(U//FOUO) Management Response: The Director, COMM concurred with this recommendation. A complete copy of the management comments is included in Appendix F.

(U) Other Matter

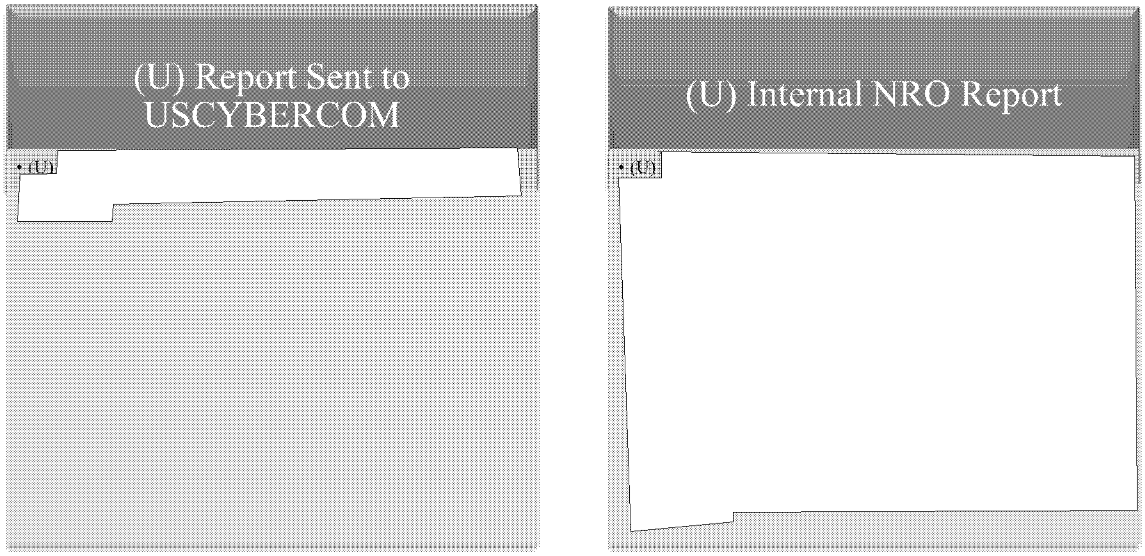
(S//NF) The OIG noted inconsistencies with the [redacted] external cyber incidents reports the NRO submitted to IC SCC and USCYBERCOM. Specifically, the OIG reviewed [redacted] reports provided to the IC SCC from January 2013 through February 2014 and found that [redacted] reports included language that refers to separate incidents that are completely unrelated to the [redacted]

(b)(1)
(b)(3)

(U//FOUO) The OIG also met with USCYBERCOM representatives to determine whether they had any concerns with the cyber incident reports provided by the NRO. They acknowledged that they are satisfied with the reporting of cyber incidents provided by the NRO. However, the OIG's review of [redacted] cyber incident reports the NRO provided to USCYBERCOM between January 2013 and February 2014 showed that [redacted] omitted vital details about the cyber incidents. With that said, opportunities exist for improvement with regard to USCYBERCOM reporting.

(U//FOUO) The Chairman of the Joint Chiefs of Staff Manual 6510.01A, *Information Assurance and Computer Network Defense Volume I Incident Handling Program*, requires that cyber incident reports to USCYBERCOM contain specific technical details. However, most of the NRO cyber incidents reported to USCYBERCOM contained only a very brief description of the cyber incident, and omitted significant details that were available and should have been included. Figure 7 shows one cyber incident description in a report sent to USCYBERCOM compared to the description of the same cyber incident in an internal NRO report.

Unless noted, redactions on this page fall under Exemption (b)(3).



(U) Report Sent to USCYBERCOM

• (U) [redacted]

(U) Internal NRO Report

• (U) [redacted]

(U) Figure 7: Comparison Between USCYBERCOM and Internal Report

Figure is UNCLASSIFIED

(U//~~FOUO~~) While IC SCC and USCYBERCOM did not express concern over the information contained in the NRO cyber incident reports, this is an opportunity for the NRO to take action to increase information sharing to contribute to an IC-wide operation. [redacted]

[redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) APPENDIX A: Summary of Recommendations

(U//~~FOUO~~) Effective 15 September 2014, the Chief Information Office and Communications Systems Directorate (COMM) merged. With this merger, the Director, COMM assumed the Chief Information Officer designation. Therefore, the recommendations that were to be addressed to the CIO prior to the merger are addressed to the Director, COMM.

(U) Recommendation #1 for the Director, COMM:

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

(U) Recommendation #2 for the Director, COMM:

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

(U) Recommendation #3 for the Director, COMM:

(U//~~FOUO~~) [redacted] and ICD 502.

(U) Recommendation #4 for the Director, COMM:

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

(U) Recommendation #5 for the Director, OS&CI:

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

(U) Recommendation #6 for the Director, COMM:

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

(U) Recommendation #7 for the Director, COMM:

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

(U) Recommendation #8 for the Director, COMM:

(U//FOUO) [redacted]

(U) Recommendation #9 for the Director, COMM:

(U//FOUO) [redacted]

(b)(3)

(U) Recommendation #10 for the Director, COMM:

(U//FOUO) [redacted]

(U) APPENDIX B: Policies Related to Computer Network Defense

(U) Table 1. Computer Network Defense Policies

Organization	Description of Policies
Federal Laws	• The *Federal Information Security Management Act of 2002* requires each agency to develop and implement an agency-wide information security program that includes procedures for detecting, reporting, and responding to security incidents. • National Security Presidential Directive-54/Homeland Security Presidential Directive-23, *Cybersecurity Policy*, requires agencies to increase efforts to coordinate and enhance the security of their classified and unclassified networks; increase protection of the data on these networks; and improve their capability to deter, detect, prevent, protect against, and respond to threats against information systems and data.
Director of National Intelligence (DNI)	• Intelligence Community Directive (ICD) 502, *Integrated Defense of the IC Information Environment*, identifies the organizations engaged in computer network defense (CND) of the IC Information Environment and specifies their roles and responsibilities. • Intelligence Community Standard (ICS) 502-01, *Computer Incident Response and Computer Network Defense,* defines the baseline computer incident response responsibilities, capabilities, and supporting CND services in the intelligence community. • *Intelligence Community Incident Reporting Procedures* provides reporting procedures for cyber security incidents, events, outages, and data spillages, in support of ICD 502. • *Intelligence Community Information Assurance Architecture* describes information assurance (IA) capabilities necessary to provide agencies with the ability to counter increasingly sophisticated cyber threats. • *Detailed Plan to Increase the Security of Classified Networks*, details enterprise cybersecurity capabilities that include processes and services that enhance the security and situational awareness of classified networks.

Department of Defense (DoD)	• DoD Directive 8500.1, *Information Assurance*, requires a defense-in-depth approach to IA and to make appropriate use of IA infrastructures, including incident response. • DoD Directive 8530.1, *Computer Network Defense*, requires all DoD information systems and computer networks to be monitored in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security or function of DoD operations, DoD information systems or computer networks. • DoD Instruction 8500.2, *Information Assurance Implementation*, requires Heads of DoD Components to provide for vulnerability mitigation and an incident response and reporting capability. • Chairman of the Joint Chiefs of Staff Manual 6510.01 describes the DoD Incident Handling Program, the major processes that take place within the incident handling program, and the interactions with related U.S. Government computer network defense activities.
National Reconnaissance Office (NRO)	• Corporate Business Process (CBP) 50, *Information Technology, Information Assurance, and Information Management*, directs the NRO to establish an Information Assurance Program including cyber incident detection and response capabilities. • Corporate Business Process Instruction (CBPI) 50-2E, *Enterprise Defense – Cyber Incident Response,* implements the cyber incident prevention and detection requirements outlined in CBP 50. These requirements include procedures to assess the damage and minimize the impact of cyber incidents, provide data to identify system vulnerabilities, and improve enterprise defenses and countermeasures. • NRO Directive (ND) 52-15, *Risk and Vulnerability Assessments, Reviews, and Updates*, directs the NRO to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems. This includes the [redacted] [redacted] roles and responsibilities, to include coordinating the assessment, prioritization, and remediation of vulnerabilities. • NRO [redacted] *Concept of Operations*, outlines the process for the NRO to coordinate and leverage resources within the existing directorates and offices to establish the framework for an NRO Information Enterprise critical incident response and reporting capability.

(b)(3)

National Institute for Standards and Technology (NIST)	• NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, seeks to assist organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidance on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents. • NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems*, assists organizations in understanding intrusion detection system and intrusion prevention system technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems.

Table is U//~~FOUO~~

PAGE INTENTIONALLY LEFT BLANK

(b)(1)
(b)(3)

Unless noted, redactions on this page fall under Exemption (b)(3).

Page Denied

PAGE INTENTIONALLY LEFT BLANK

(U) APPENDIX D: NRO Cyber Incident Events and Categories

(U) Table 1. NRO Cyber Incident Events and Categories

Category	Description
1 [Reportable]	**Root Level Intrusion:** Unauthorized privileged access (administrative or root access) to a system.
2 [Reportable]	**User Level Intrusion:** Unauthorized non-privileged access (user-level permission) to a system. Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges.
3 [Non-reportable]	**Unsuccessful Activity Attempt:** Attempt to gain unauthorized access to a system, which is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (i.e., attacker attempted valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Can include reporting of quarantined malicious code.
4 [Reportable]	**Denial of Service:** Activity that impairs, impedes, or halts the normal functionality of a system or network.
5 [Non-reportable]	**Non-Compliance Activity:** This category is used for activity that due to actions (either via configuration or usage), makes systems potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliance or improper configuration changes or improper handling by authorized users.
6 [Non-reportable]	**Reconnaissance:** An activity (scan/probe) that seeks to identify a computer, an open port, an active service, or any combination thereof for later exploit. This activity does not directly result in a compromise.
7 [Reportable]	**Malicious Logic:** Installation of malicious software (e.g., Trojan, backdoor, virus, worm, etc.).
8 [Initial]	**Investigating:** Activities that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No incident will be closed out as a category 8.
9 [Non-reportable]	**Explained Anomaly:** Activities that are initially suspected as being malicious in nature but after investigation, are determined not to fit the criteria for any of the other categories (e.g., systems malfunction, false positive, bad information, etc.).
10 [Non-reportable]	**Misuse/Porn:** Activities that are in breach of best security practices, NRO Acceptable Use Policy and/or contain blatant pornographic activity.

Table is UNCLASSIFIED

PAGE INTENTIONALLY LEFT BLANK

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) APPENDIX E: Cyber Incident Details

(U) Network Security Assessment

~~(S//TK//NF)~~ [redacted] (b)(1) (b)(3)

~~(S//NF)~~ [redacted]

[24] ~~(S//TK//NF)~~ [redacted] (b)(1) (b)(3)

[25] (U) [redacted]

(b)(1)
(b)(3)

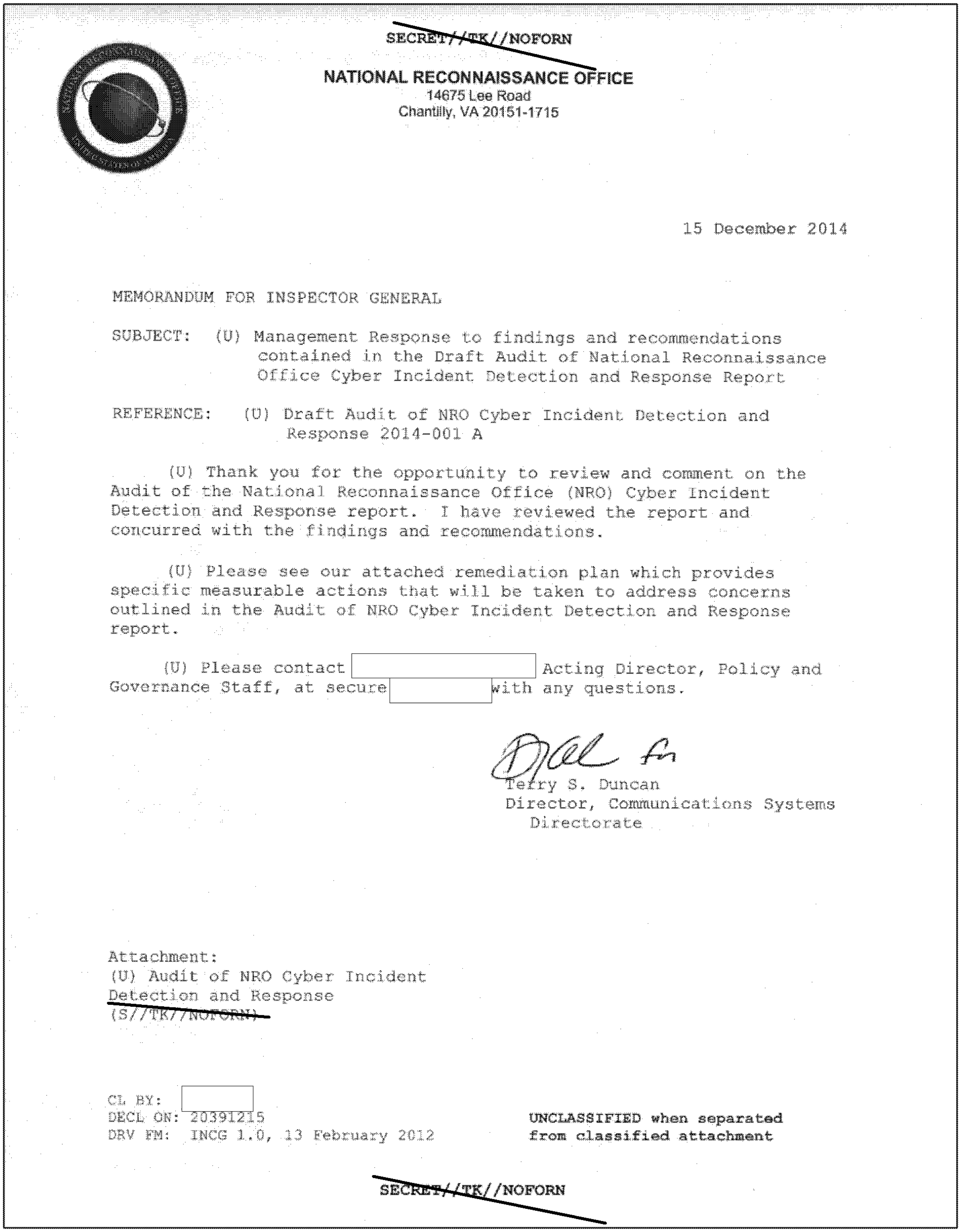
Page Denied

(b)(1)
(b)(3)

Page Denied

PAGE INTENTIONALLY LEFT BLANK

(U) APPENDIX F: Management Comments



~~SECRET//TK//NOFORN~~

NATIONAL RECONNAISSANCE OFFICE
14675 Lee Road
Chantilly, VA 20151-1715

15 December 2014

MEMORANDUM FOR INSPECTOR GENERAL

SUBJECT: (U) Management Response to findings and recommendations contained in the Draft Audit of National Reconnaissance Office Cyber Incident Detection and Response Report

REFERENCE: (U) Draft Audit of NRO Cyber Incident Detection and Response 2014-001 A

(U) Thank you for the opportunity to review and comment on the Audit of the National Reconnaissance Office (NRO) Cyber Incident Detection and Response report. I have reviewed the report and concurred with the findings and recommendations.

(U) Please see our attached remediation plan which provides specific measurable actions that will be taken to address concerns outlined in the Audit of NRO Cyber Incident Detection and Response report.

(U) Please contact [redacted] Acting Director, Policy and Governance Staff, at secure [redacted] with any questions.

Terry S. Duncan
Director, Communications Systems
Directorate

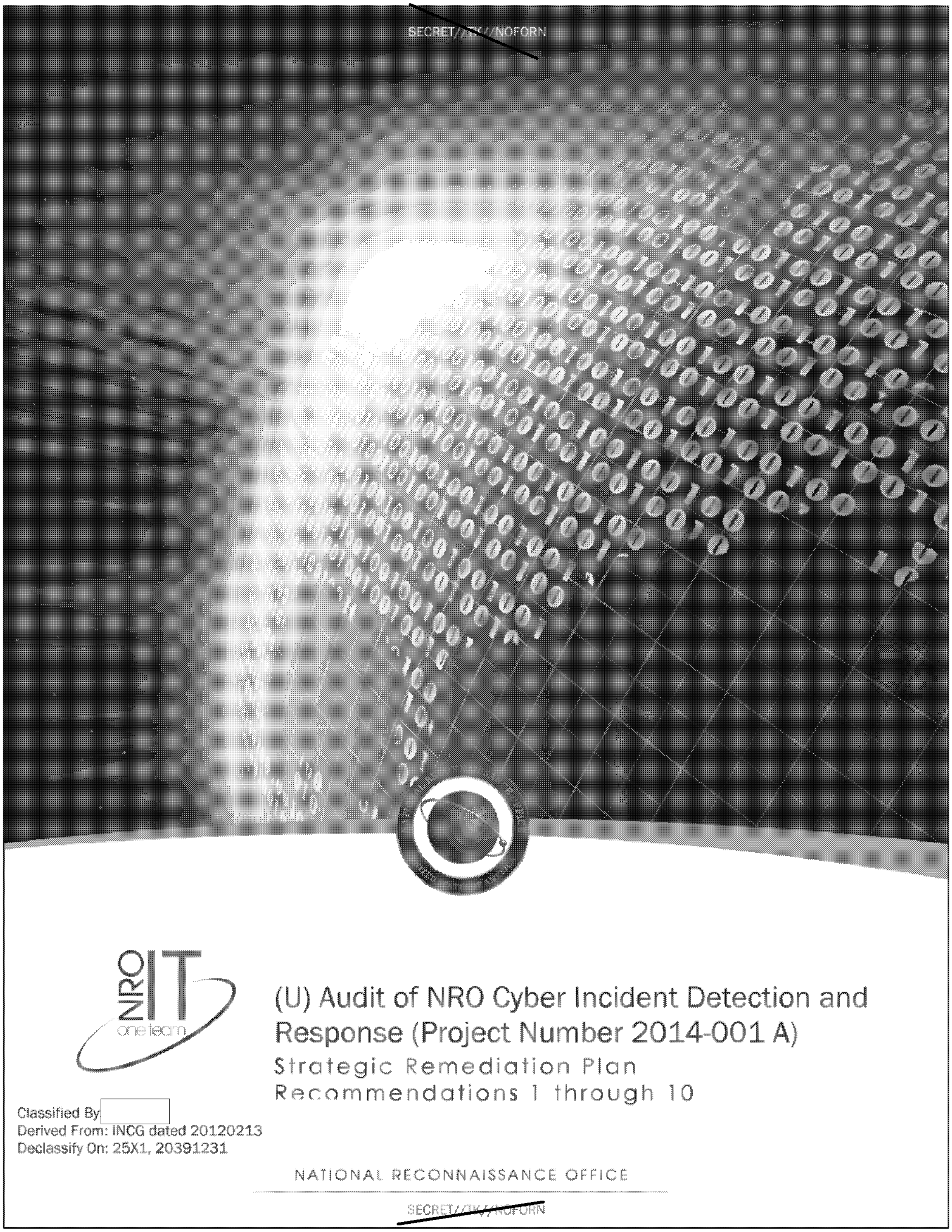
Attachment:
(U) Audit of NRO Cyber Incident
Detection and Response
~~(S//TK//NOFORN)~~

CL BY: [redacted]
DECL ON: 20391215
DRV FM: INCG 1.0, 13 February 2012

UNCLASSIFIED when separated from classified attachment

~~SECRET//TK//NOFORN~~

Unless noted, redactions on this page fall under Exemption (b)(3).



~~SECRET//TK//NOFORN~~

(U) Audit of NRO Cyber Incident Detection and Response (Project Number 2014-001 A)

Strategic Remediation Plan Recommendations 1 through 10

Classified By [redacted]
Derived From: INCG dated 20120213
Declassify On: 25X1, 20391231

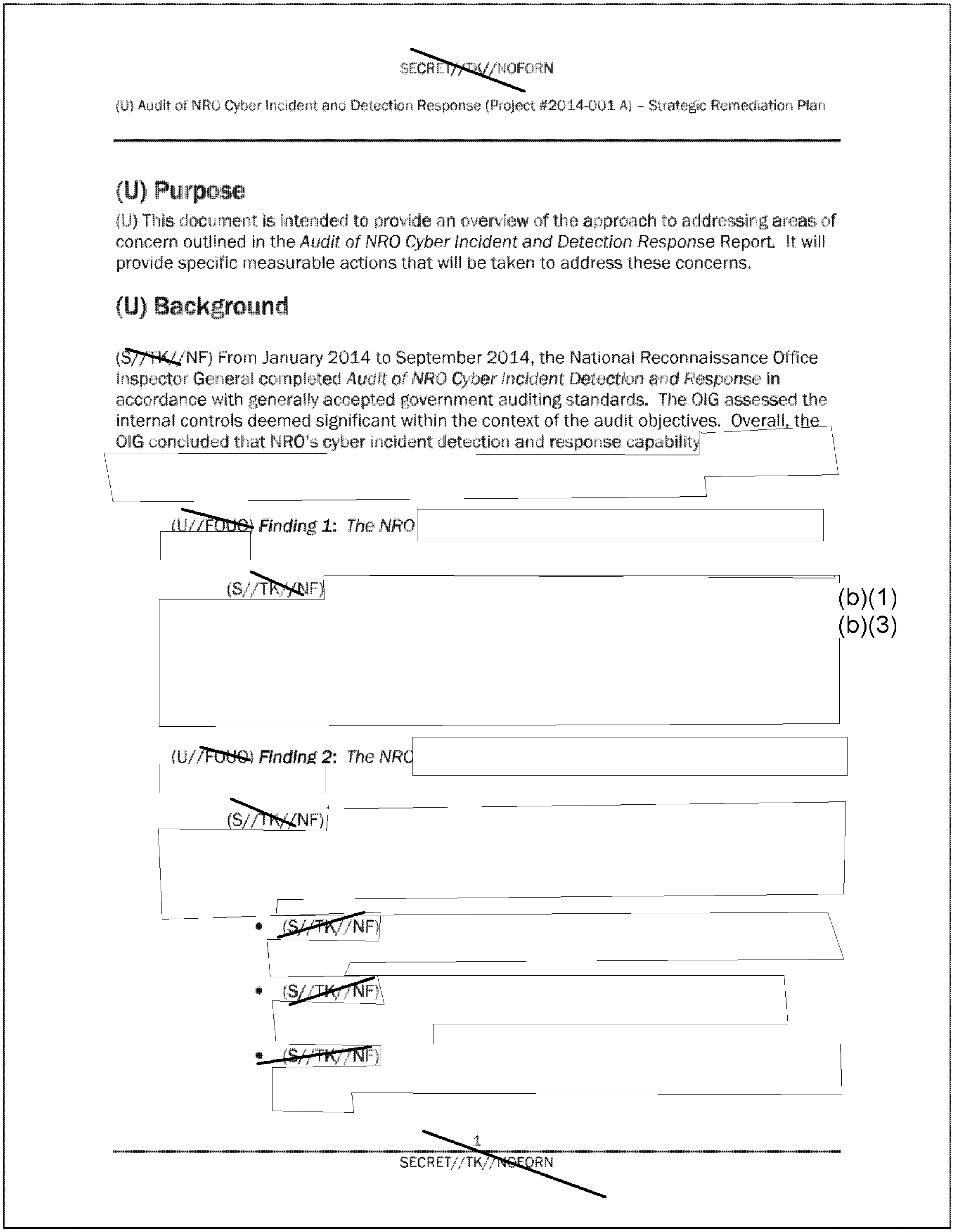
NATIONAL RECONNAISSANCE OFFICE

~~SECRET//TK//NOFORN~~

Unless noted, redactions on this page fall under Exemption (b)(3).

Contents

Unless noted, redactions on this page fall under Exemption (b)(3).



(U) Purpose

(U) This document is intended to provide an overview of the approach to addressing areas of concern outlined in the *Audit of NRO Cyber Incident and Detection Response* Report. It will provide specific measurable actions that will be taken to address these concerns.

(U) Background

~~(S//TK//NF)~~ From January 2014 to September 2014, the National Reconnaissance Office Inspector General completed *Audit of NRO Cyber Incident Detection and Response* in accordance with generally accepted government auditing standards. The OIG assessed the internal controls deemed significant within the context of the audit objectives. Overall, the OIG concluded that NRO's cyber incident detection and response capability [redacted]

(b)(1)
(b)(3)

~~(U//FOUO)~~ ***Finding 1**: The NRO* [redacted]

~~(S//TK//NF)~~ [redacted]

(b)(1)
(b)(3)

~~(U//FOUO)~~ ***Finding 2**: The NRO* [redacted]

~~(S//TK//NF)~~ [redacted]

(b)(1)
(b)(3)

- ~~(S//TK//NF)~~ [redacted]
- ~~(S//TK//NF)~~ [redacted]
- ~~(S//TK//NF)~~ [redacted]

(b)(1)
(b)(3)

Page Denied

Unless noted, redactions on this page fall under Exemption (b)(3).

6. (U//~~FOUO~~) [redacted]

7. (U//~~FOUO~~) [redacted]

8. (U//~~FOUO~~) [redacted]

9. (U//~~FOUO~~) [redacted]

10. (U//~~FOUO~~) [redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) Activities, Milestones, Risks and Dependencies

The following section provides specific milestones and deliverables related to each of the recommendations included in the audit report.

(U) Finding 1: The NRO [redacted] [redacted]

(U//~~FOUO~~) Recommendation 1: [redacted]

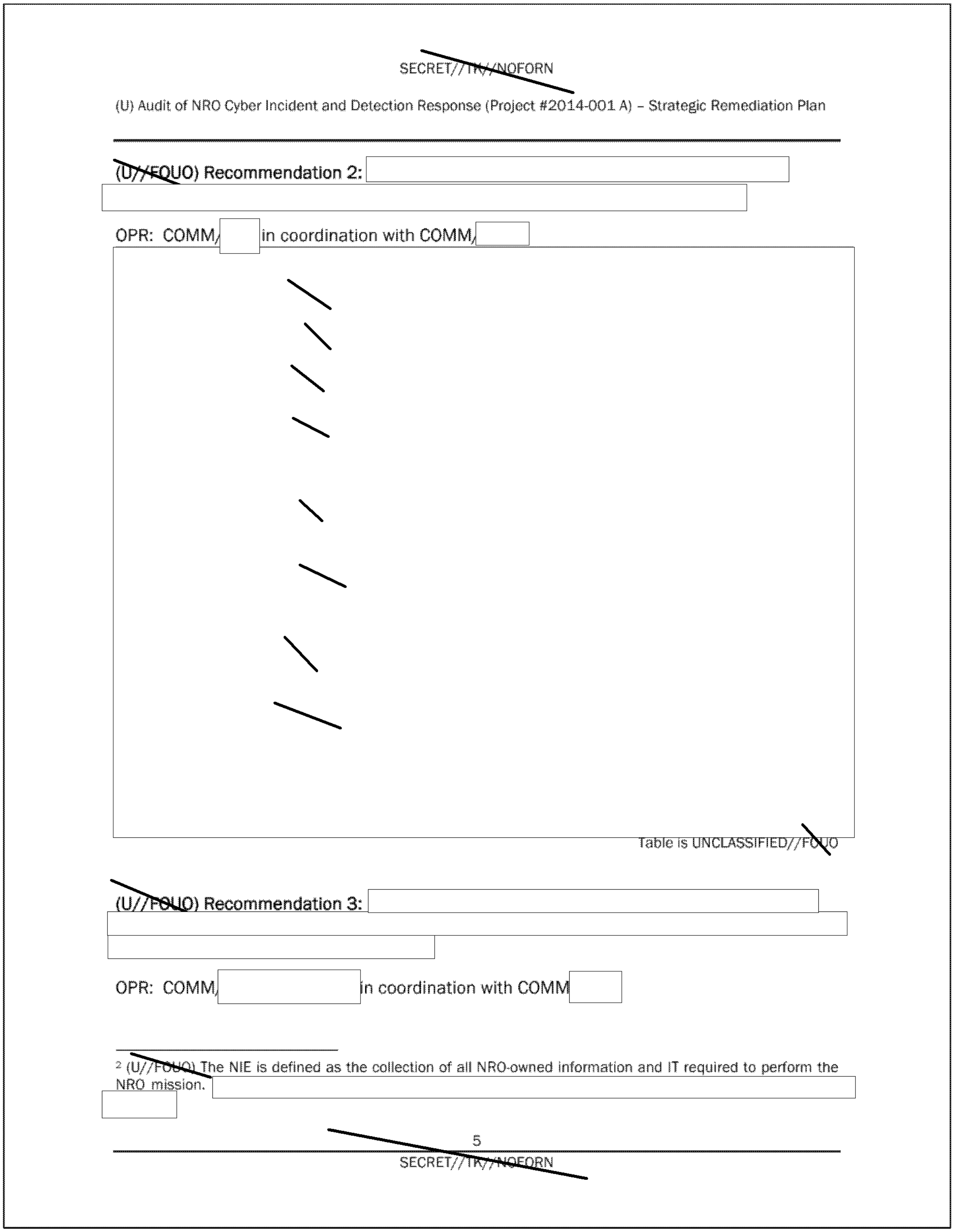
OPR: COMM [redacted] in coordination with COMM [redacted]

[redacted]

Table is UNCLASSIFIED//~~FOUO~~

[1] (U) Collection of interconnected components, based on a coherent security architecture and design. May include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. [CNSSI 4009]

Unless noted, redactions on this page fall under Exemption (b)(3).



~~(U//FOUO)~~ Recommendation 2: [redacted]

OPR: COMM/[redacted] in coordination with COMM/[redacted]

[redacted]

Table is UNCLASSIFIED//~~FOUO~~

~~(U//FOUO)~~ Recommendation 3: [redacted]

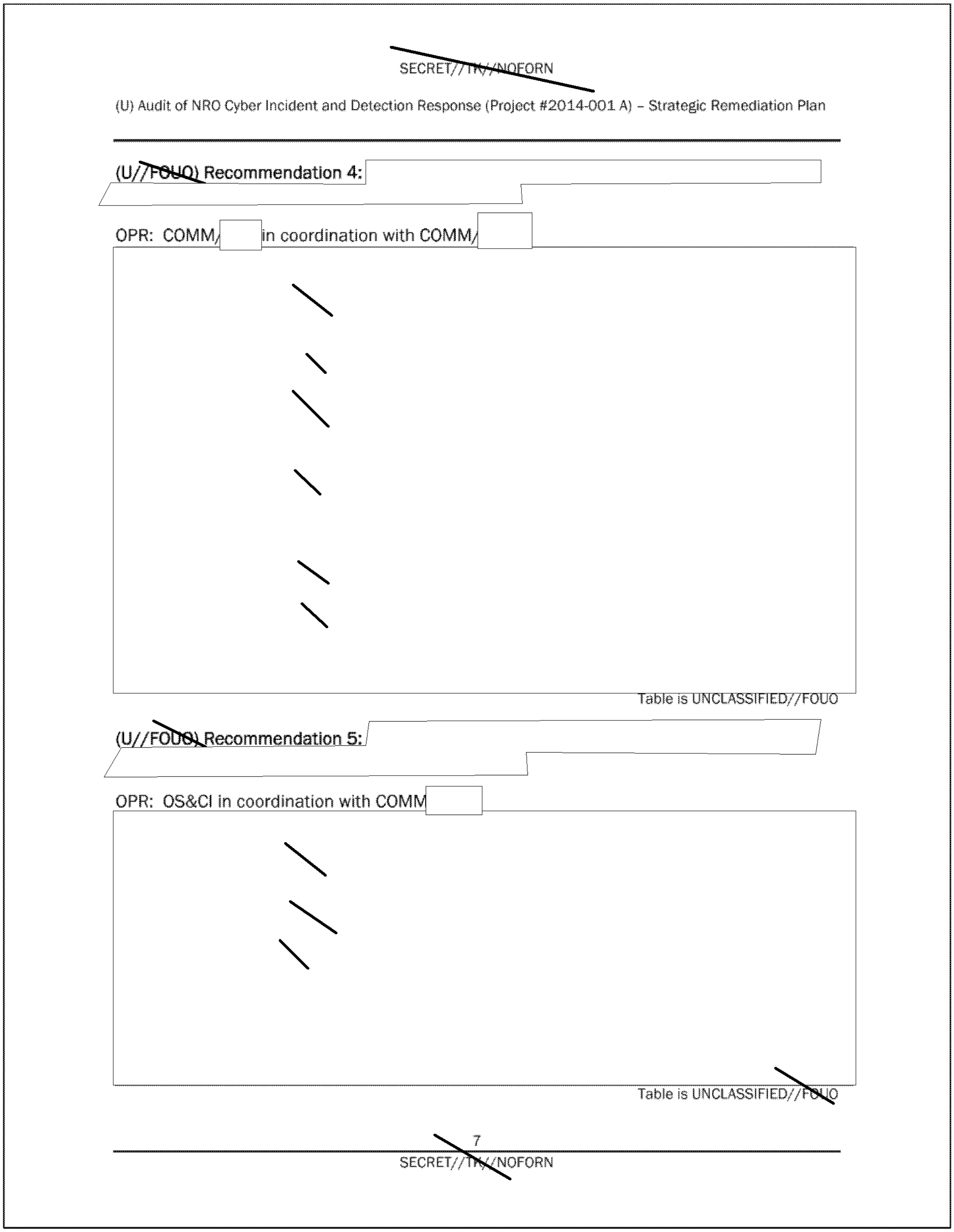
OPR: COMM/[redacted] in coordination with COMM[redacted]

[2] ~~(U//FOUO)~~ The NIE is defined as the collection of all NRO-owned information and IT required to perform the NRO mission. [redacted]

Unless noted, redactions on this page fall under Exemption (b)(3).

Page Denied

Unless noted, redactions on this page fall under Exemption (b)(3).



~~(U//FOUO)~~ Recommendation 4: [redacted]

OPR: COMM/[redacted] in coordination with COMM/[redacted]

[redacted]

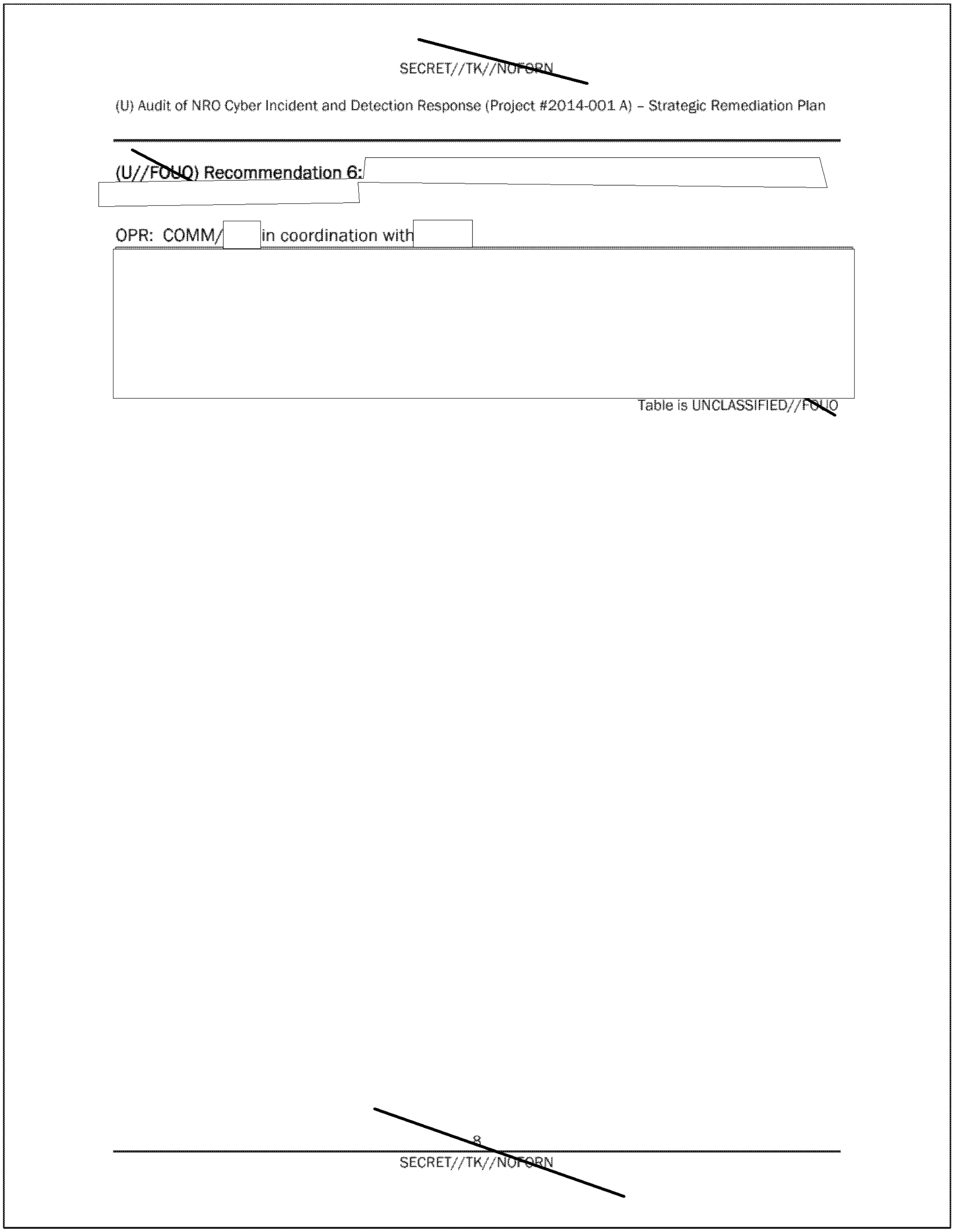
Table is UNCLASSIFIED//FOUO

~~(U//FOUO)~~ Recommendation 5: [redacted]

OPR: OS&CI in coordination with COMM[redacted]

[redacted]

Table is UNCLASSIFIED//~~FOUO~~



~~SECRET//TK//NOFORN~~

(U) Audit of NRO Cyber Incident and Detection Response (Project #2014-001 A) – Strategic Remediation Plan

(U//~~FOUO~~) Recommendation 6: [redacted]

OPR: COMM/[redacted] in coordination with [redacted]

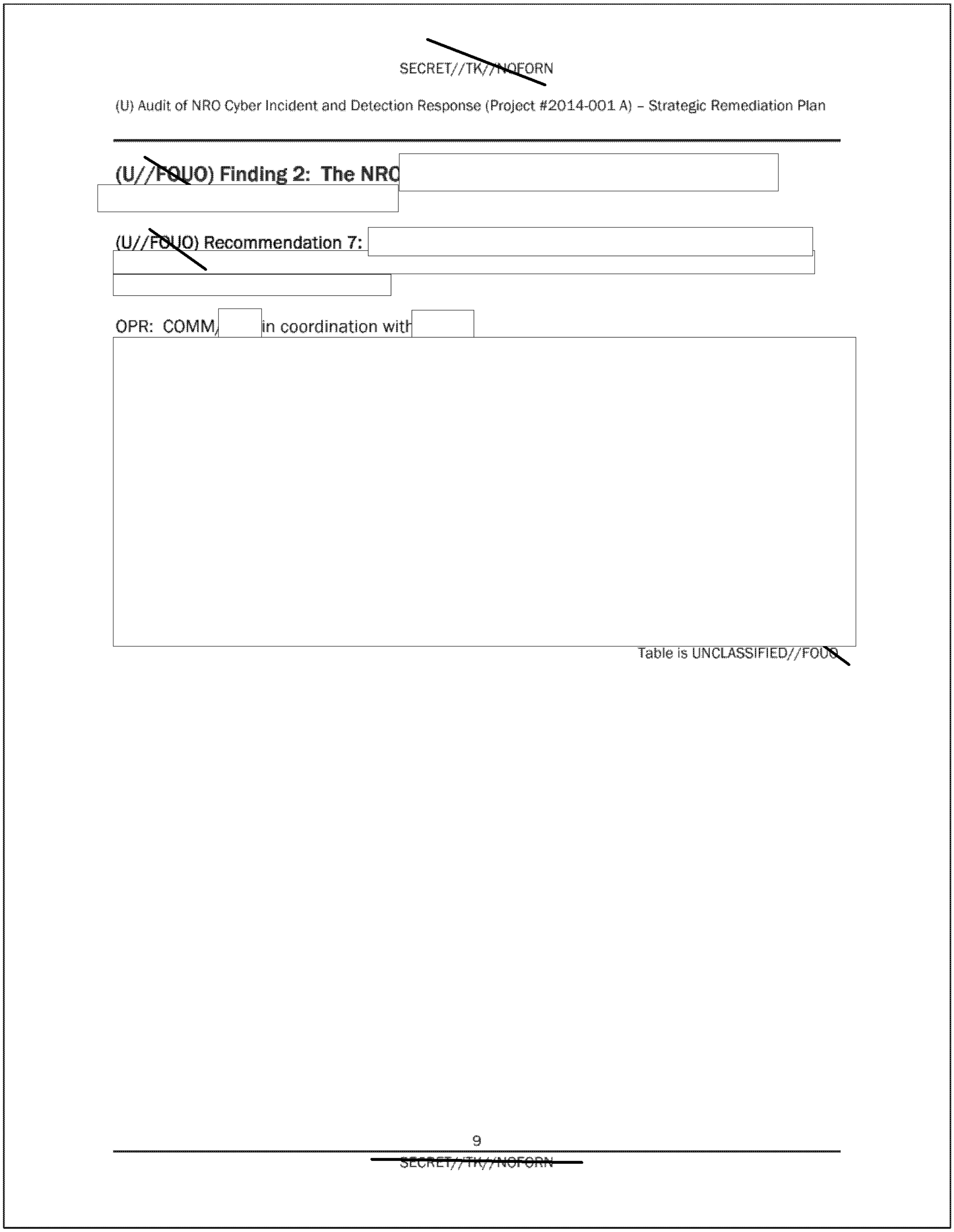
[redacted]

Table is UNCLASSIFIED//~~FOUO~~

8

~~SECRET//TK//NOFORN~~

Unless noted, redactions on this page fall under Exemption (b)(3).



(U//~~FOUO~~) Finding 2: The NRO [redacted]

(U//~~FOUO~~) Recommendation 7: [redacted]

OPR: COMM/[redacted] in coordination with [redacted]

[redacted]

Table is UNCLASSIFIED//~~FOUO~~

Unless noted, redactions on this page fall under Exemption (b)(3).

Page Denied

Unless noted, redactions on this page fall under Exemption (b)(3).

Page Denied

Unless noted, redactions on this page fall under Exemption (b)(3).

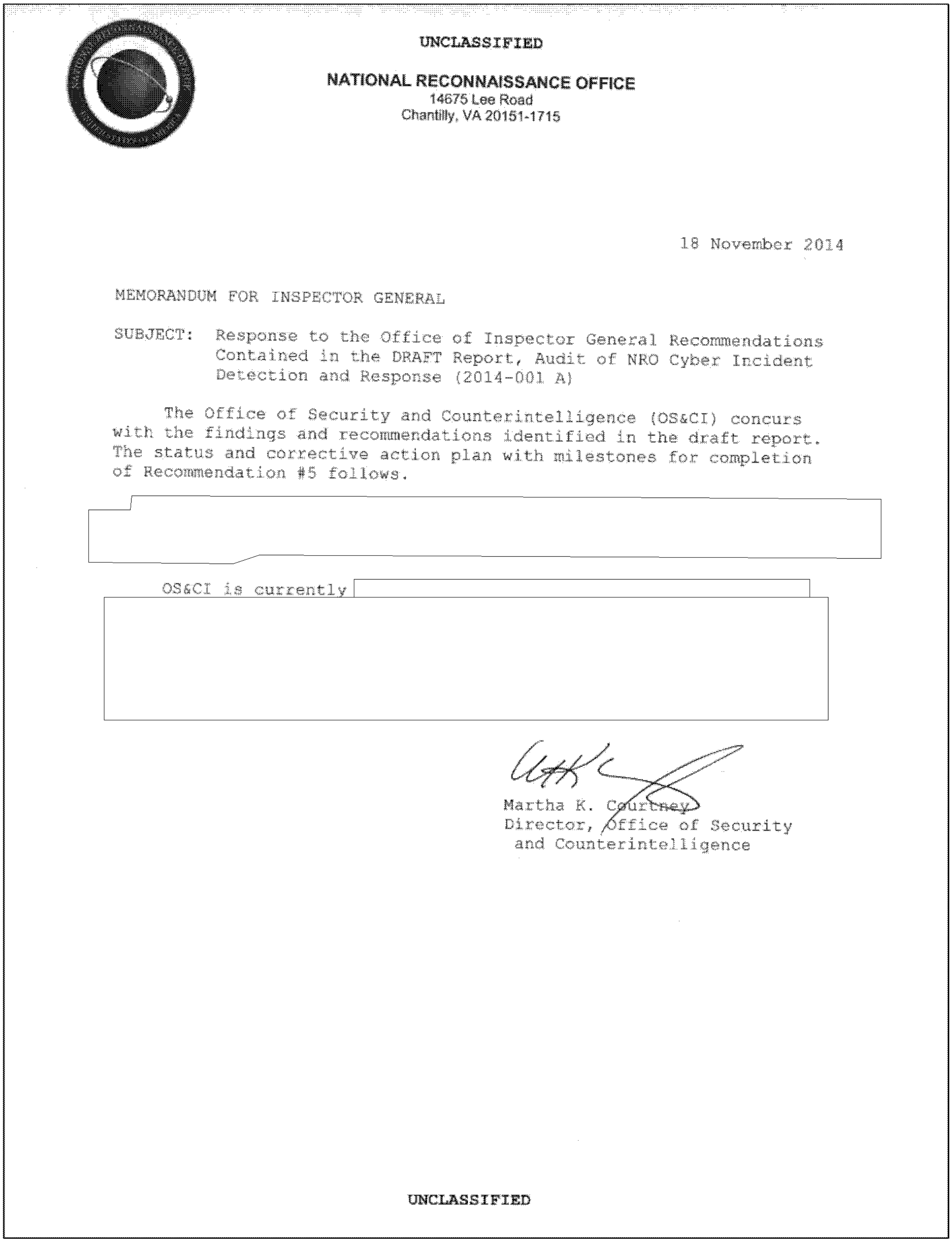
(U//~~FOUO~~) Finding 3: NRO Cyber Incidents [redacted] [redacted]

(U//~~FOUO~~) Recommendation 10: [redacted] [redacted]

OPR: COMM/[redacted] in coordination with COMM/[redacted] and COMM/[redacted]

[redacted]

Table is UNCLASSIFIED//~~FOUO~~



UNCLASSIFIED

NATIONAL RECONNAISSANCE OFFICE
14675 Lee Road
Chantilly, VA 20151-1715

18 November 2014

MEMORANDUM FOR INSPECTOR GENERAL

SUBJECT: Response to the Office of Inspector General Recommendations Contained in the DRAFT Report, Audit of NRO Cyber Incident Detection and Response (2014-001 A)

The Office of Security and Counterintelligence (OS&CI) concurs with the findings and recommendations identified in the draft report. The status and corrective action plan with milestones for completion of Recommendation #5 follows.

[redacted]

OS&CI is currently [redacted]

(b)(3)

Martha K. Courtney
Director, Office of Security
and Counterintelligence

UNCLASSIFIED

Unless noted, redactions on this page fall under Exemption (b)(3).

(U) APPENDIX G: Major Contributors to this Report

[redacted]

Assistant Inspector General for Audits

Deputy Assistant Inspector General for Information Technology Audits

Auditor-in-Charge

Auditor-in-Charge

Auditor

Quality Assurance Reviewer

Quality Assurance Reviewer

Writing Facilitator