

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: **<http://www.theblackvault.com>**



NATIONAL RECONNAISSANCE OFFICE

14675 Lee Road
Chantilly, VA 20151-1715

25 May 2017

Mr. John Greenewald, Jr.
[REDACTED]

REF: FOIA Cases F-2017-00045

Dear Mr. Greenewald:

This is in response to your request dated 6 January 2017 and received by the National Reconnaissance Office (NRO) on 9 January 2017. Pursuant to the Freedom of Information Act (FOIA), you requested a copy of "the NRO/OIG Investigation, labeled as, 'Audit of the National Reconnaissance Office [REDACTED]' closed April 30, 2015...referenced in...F-2016-00055."

Your request has been processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. A thorough search of our files and databases located one document responsive to your request. This document is being released to you in part.

Material redacted is denied pursuant to FOIA exemptions:

(b)(1), as information that is properly classified pursuant to Executive Order 13526, Sections 1.4(c) and 1.4(g); and

(b)(3), which is the basis for withholding information exempt from disclosure by statute. The relevant withholding statute is 10 U.S.C. § 424, which provides (except as required by the President or for information provided to Congress), that no provision of law shall be construed to require the disclosure of the organization or any function of the NRO; the number of persons employed by or assigned or detailed to the NRO; or the name or official title, occupational series, grade, or salary of any such person.

You have the right to appeal this determination to the NRO Appellate Authority, 14675 Lee Road, Chantilly, VA 20151-1715, within 90 days of the above date. You may also submit an appeal electronically by completing the form available on the NRO's public web site at <http://www.nro.gov/foia/AppealInput.aspx>. Please include an explanation of the reason(s) for your appeal as part of your submission. The FOIA also provides that you may seek dispute resolution for any adverse determination through the NRO FOIA Public Liaison and/or through the Office of Government Information Services (OGIS). Please refer to the OGIS public web page at <https://ogis.archive.gov/> for additional information.

If you have any questions, please call the Requester Service Center at (703) 227-9326 and reference case number **F-2017-00045**.

Sincerely,

A handwritten signature in cursive script, appearing to read "Patricia B. Camerese".

Patricia B. Camerese
FOIA Public Liaison

Enclosure: Audit of the...Insider Threat Program

~~SECRET//NOFORN~~**NATIONAL RECONNAISSANCE OFFICE***Office of Inspector General**14675 Lee Road**Chantilly, VA 20151-1715*

30 April 2015

MEMORANDUM FOR DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
PRINCIPAL DEPUTY DIRECTOR, NATIONAL RECONNAISSANCE
OFFICE
DEPUTY DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTOR, OFFICE OF SECURITY AND COUNTERINTELLIGENCE

SUBJECT: (U) Memorandum Report: Audit of the National Reconnaissance
Office Insider Threat Program (Project Number 2015-002 A)

(U) The National Reconnaissance Office (NRO) Office of Inspector
General (OIG) Memorandum Report on the *Audit of the NRO Insider Threat
Program* is attached. The OIG conducted the survey phase of this audit
from December 2014 to April 2015 in accordance with government
auditing standards.

~~S//NF~~

(U//~~FOUO~~) The objective of this audit was to determine whether
the NRO has adequate controls in place to prevent and detect insider
threats against NRO networks, systems, and data. After the OIG
announced this audit, Office of Security and Counterintelligence
(OS&CI) leadership [redacted]

[redacted] The OIG performed
the survey phase of this audit, [redacted]

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

[redacted] Overall, the OS&CI agreed with the OIG's
findings.

~~S//NF~~

(U//~~FOUO~~) Because the OIG and NRO leadership consider insider
threat to be a high risk area, the OIG will include an audit of the
NRO Insider Threat Program as part of the OIG Fiscal Year 2016 annual
work plan. The audit will include [redacted]
the attached report. [redacted]

(b)(3)

[redacted] external assessments of
the program.

~~SECRET//NOFORN~~~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~


Approved for Release: 2017/05/25 C05099124
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

SUBJECT: (U) Memorandum Report: Audit of the National Reconnaissance
Office Insider Threat Program (Project Number 2015-002 A)

(U) I appreciate the courtesies extended to my staff during this
audit. Please direct any questions you may have regarding this
memorandum to [redacted], Auditor-In-Charge, at [redacted]
(secure), or [redacted], Deputy Assistant Inspector General, at
[redacted] (secure).

(b)(3)


Adam G. Harris
Inspector General

cc:
D/COMM
D/MS&O
D/MOD
D/OC
GC
D/OSHC

Attachment:

(U) Memorandum Report (U//~~FOUO~~)

~~SECRET//NOFORN~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Approved for Release: 2017/05/25 C05099124

Approved for Release: 2017/05/25 C05099124
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

SUBJECT: (U) Memorandum Report: Audit of the National Reconnaissance
Office Insider Threat Program (Project Number 2015-002 A)

OIG/ [] [] [] /30 Apr 15

(b)(3)

DISTRIBUTION:

Hard copy

Director, National Reconnaissance Office
Principal Deputy Director, National Reconnaissance Office
Deputy Director, National Reconnaissance Office
Director, Communications Systems Directorate and Chief Information
Officer
Director, Management Services and Operations Directorate
Director, Mission Operations Directorate
Director, Office of Contracts
General Counsel
Director, Office of Security and Counterintelligence
Director, Office of Strategic Human Capital
Auditor-In-Charge []
Follow-up Administrator []
OIG Chron

(b)(3)

(b)(3)

Soft copy

IG-Followup-Tracker (TIER)

~~SECRET//NOFORN~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Approved for Release: 2017/05/25 C05099124

Approved for Release: 2017/05/25 C05099124
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~SECRET//NOFORN~~

OFFICE OF INSPECTOR GENERAL

(U) Audit of the National Reconnaissance Office Insider Threat Program (Project Number 2015-002 A)

(U) Introduction

(U) The Intelligence Community (IC) defines the term *insider threat* as an insider using her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. As recently experienced by the IC and the Department of Defense, this harm can take many forms, including industrial espionage, unauthorized disclosure of classified information, or even violent acts. This is an organization-wide risk that is not limited to information technology or counterintelligence (CI).

(U) To address the magnitude of this risk, in October 2011, the President released an Executive Order (E.O.)¹ requiring departments and agencies to establish an insider threat program. The President subsequently issued several additional memoranda² that established the National Insider Threat Policy clarifying his expectations for protecting federal entities. Under Presidential direction, the National Insider Threat Task Force (NITTF) issued guidance on how to comply with the National Insider Threat Policy and specified what must be included in an insider threat program. It prescribed a coordinated effort across multiple disciplines. Examples of these disciplines include Personnel Security, Law Enforcement, Privacy and Civil Liberties, Human Resources, Information Assurance, CI, and Office of Inspector General (OIG). These interrelated disciplines are supposed to form an agency-wide safety net, including government and contractors, to deter, detect, and mitigate actions by employees who may represent a threat to national security.

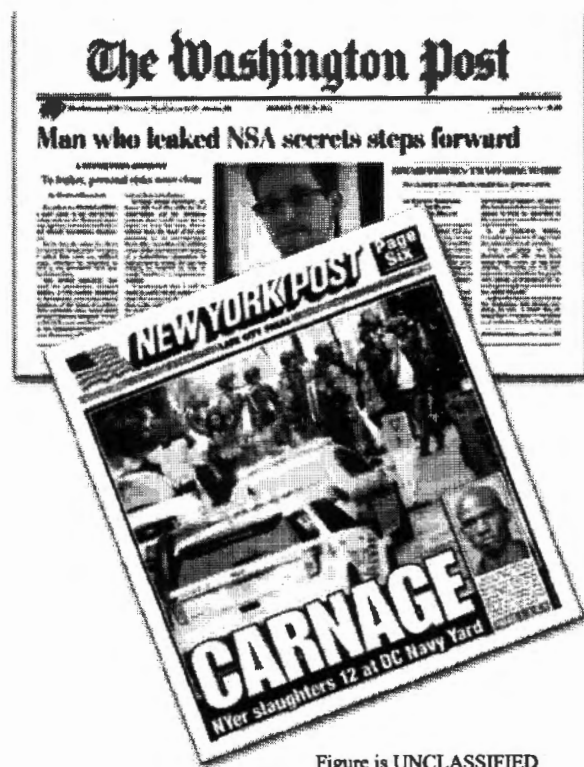


Figure is UNCLASSIFIED

(U) Accepting that an insider threat program takes time to mature, the President provided a timeline for agencies to reach initial operating capability with their respective Insider Threat

¹ (U) E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*

² (U) White House Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, and White House Memorandum, *Compliance with the President's National Insider Threat Policy*

~~SECRET//NOFORN~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Programs. The NITTF, with White House concurrence, clarified that by 20 May 2013, all agencies must

1. (U) designate an insider threat senior official(s),
2. (U) issue an insider threat policy signed by the department or agency head, and
3. (U) submit to department or agency leadership an insider threat program implementation plan that addresses how the organization intends to meet the requirements set forth in the minimum standards.

(U) Scope and Methodology

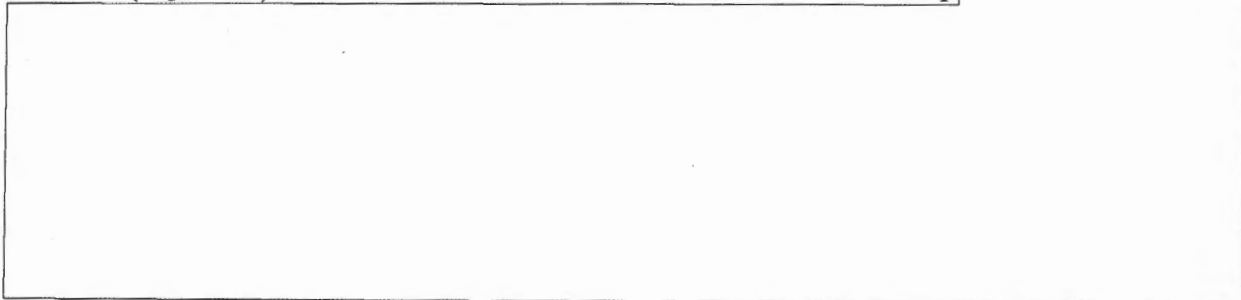
(U//~~FOUO~~) The OIG conducted the survey phase of this audit from December 2014 to April 2015 in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions. During this phase of the audit, the OIG met with personnel from the Office of Security and Counterintelligence (OS&CI) and other Insider Threat Program stakeholders including the Communications Systems Directorate, Mission Support and Operations Directorate, Office of General Counsel, and Office of Strategic Human Capital, and reviewed documentation. The OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

(U) Results

~~S//NF~~

(U//~~FOUO~~) After the OIG announced this audit, OS&CI leadership

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



~~S//NF~~

(U//~~FOUO~~)

in the NRO Insider Threat Program

(b)(1)

~~S//NF~~



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

~~SECRET//NOFORN~~

Approved for Release: 2017/05/25 C05099124
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~SECRET//NOFORN~~

(b)(3)

~~S//NF~~

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

(U) Recommendation #1 for the Director, OS&CI:

(b)(3)

(U)

~~S//NF~~

~~(U//FOUO)~~ The OIG obtained and reviewed the existing NRO Insider Threat Program

(b)(3)

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

~~S//NF~~

~~(U//FOUO)~~

element of an insider threat program, the

(b)(3)

OIG is

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

efforts across many disciplines to fulfill this mission.

~~S//NF~~

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

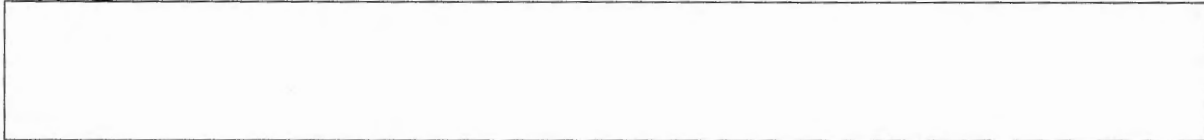
~~SECRET//NOFORN~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

criteria not only requires a plan to be built reflecting a multidisciplinary approach, but it also requires that the plan provide the organization with a detailed way forward and include the following program management elements:

- (U) Tasks required to accomplish program goals, and assignment of responsibility for those tasks;
- (U) Task schedules and milestones;
- (U) Funding and resource allocation; and
- (U) Schedule for reporting progress, dependencies, and issues.

~~S//NF~~(b)(1)
(b)(3)

(U) Recommendation #2 for the Director, OS&CI:

~~S//NF~~

(U//~~FOUO~~) In coordination with NRO stakeholders,

maintaining the NRO Insider Threat Program, in accordance with NITTF and IC requirements.

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

(U//~~FOUO~~) memorandum report and the inherent risk that insiders pose, the OIG will include an audit of the NRO Insider Threat Program as part of the OIG Fiscal Year 2016 Annual Work Plan. The audit will include

(b)(3)

(b)(3)