NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY
HOMELAND SECURITY DIGITAL LIBRARY
SECURING THE HOMELAND THROUGH THE POWER OF INFORMATION

February 2, 2017

Improving Security and Efficiency at OPM and the National Background Investigations Bureau

Committee on Oversight and Government Reform, United States House of Representatives, One Hundred Fifteenth Congress, First Session

---

HEARING CONTENTS:

Witnesses

Kathleen McGettigan
Acting Director
Office of Personnel Management
[View Testimony]

Cord Chase
Chief Information Security Officer
Office of Personnel Management
[View Testimony]

Charles Phalen
Director
National Background Investigations Bureau
[View Testimony]

David DeVries
Chief Information Officer
National Background Investigations Bureau
[View Testimony]

Terry Halvorsen
Chief Information Officer
U.S. Department of Defense
[View Testimony]

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY
HOMELAND SECURITY DIGITAL LIBRARY
SECURING THE HOMELAND THROUGH THE POWER OF INFORMATION

Available Webcast(s)*:

[Watch Full Hearing]

Compiled From*:

https://oversight.house.gov/hearing/improving-security-efficiency-opm-national-background-investigations-bureau-2/

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

STATEMENT OF
KATHLEEN MCGETTIGAN
ACTING DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

Improving Security and Efficiency at OPM and the National Background Investigations Bureau

---

February 2, 2017

Chairman Chaffetz, Ranking Member Cummings and Members of the Committee:

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for the opportunity for myself and my colleagues with me today to testify before the committee on the National Background Investigations Bureau (NBIB) transition, the security clearance process, and information technology (IT) security. As the Acting Director of the U.S. Office of Personnel Management (OPM), I can assure you we recognize how critical this is to the Federal government and to our national security. In keeping with our focus on modernizing the way that OPM carries out its important missions, OPM has worked to optimize the business processes surrounding background investigations. OPM has also taken aggressive measures to enhance the security of its IT systems, both within the NBIB and throughout OPM, accelerating an ambitious long-term IT security and modernization plan to upgrade the security of our systems and strengthen the agency's ability to respond to cyber incidents. OPM has also partnered with the Department of Defense (DOD) and other agencies to leverage government-wide knowledge, resources, and best practices.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

The National Background Investigations Bureau

NBIB was established on October 1, 2016, and is the primary provider of background investigations for the Federal government. NBIB is designed with an enhanced focus on national security, customer service, and continuous process improvement to meet this critical government-wide need. Charles S. Phalen, Jr., the NBIB Director, has a long and distinguished career in multiple roles at senior levels in the Federal government and private industry with a focus on protecting our national security. His extensive experience includes serving in various capacities at the Central Intelligence Agency, including as the Director of Security, and with the Federal Bureau of Investigations as Assistant Director leading its Security Division.

NBIB conducts 95 percent of investigations across the government. Even those few agencies that have the statutory authority to conduct their own investigations, such as the Intelligence Community, rely on NBIB's services in some capacity. Its new organizational structure is aimed at leveraging automation, transforming business processes, and enhancing customer engagement and transparency. Through a strong partnership with DOD, NBIB will build a modern and secure IT system to comprehensively support the investigations process and enhance end-to-end processes across government. These efforts will ultimately improve the efficiency, cost effectiveness, and quality of the investigations across the Federal government.

As you are likely aware, in late 2014, OPM's market capacity for contract investigation services was drastically reduced by the loss of OPM's largest field contractor, resulting in an investigative backlog. This backlog was exacerbated by the cybersecurity incidents at OPM that were announced in 2015. Looking forward, it is an NBIB priority to address the investigative backlog while maintaining a commitment to quality and returning back to the level of performance realized from 2009 through 2014. NBIB, working with the Office of the Director of National Intelligence (ODNI), DOD and other customers, is focusing efforts in three primary areas. First and foremost, NBIB is working to increase capacity. NBIB hired 400 new Federal investigators in 2016, and NBIB recently awarded a new investigative fieldwork contract, increasing the fieldwork contractors from two companies to four. Work under the new contracts began on February 1, 2017. Second, NBIB is focusing on policy and process changes to add efficiencies, reduce level of effort, and maintain investigative quality. To support this effort, NBIB, working closely with the DOD and interagency partners, conducted a detailed business process reengineering effort and worked in collaboration with ODNI in its role as the Security Executive Agent to identify appropriate policy and process changes to help address the backlog. Third, NBIB has actively worked with customer agencies to prioritize cases and schedule those that are most critical to our national security and the mission needs of our customers.

Information technology also plays a central role in NBIB's ability to enhance the background investigation process. A key component of NBIB is to leverage DOD's cybersecurity expertise and resources to design, develop, and implement a modern and secure IT environment. While still in development, the new system, known as the National Background Investigation System (NBIS), is to be operated and maintained by DOD on behalf of NBIB. NBIB is encouraged by the significant progress DOD has made toward new capabilities that will improve the effectiveness and security of background investigations. Concurrently, the OPM Office of the Chief Information Officer (OPM CIO), in coordination with our interagency partners to include DOD and Department of Homeland Security (DHS), has aggressively pursued further improving the cybersecurity posture of the OPM network.

Role of the Office of the Chief Information Officer

OPM has worked to strengthen the infrastructure and security of not only NBIB, but also OPM's entire technology ecosystem. This effort is being led by OPM's new CIO, David DeVries, who joined OPM in September 2016. Mr. DeVries had previously been the DOD Principal Deputy CIO and has a strong relationship with his former agency that facilitates coordinating the implementation of NBIS. Indeed, as the Federal government modernizes how it does business, OPM has focused on embracing new tools and technologies to deliver optimum customer service and enhance the security of the information we house. In a rapidly changing and increasingly interconnected digital world, it is important for agencies to develop the best possible defenses and safeguards.

Over the past eight months, OPM has successfully begun to roll out its program for implementation of the Federal Information Technology Acquisition Reform Act and enhanced the agency's infrastructure in ways that will help OPM support its cybersecurity initiatives and strategies, ensure its IT programs run more efficiently and securely in supporting the OPM business lines, and better utilize limited resources.

OPM has enhanced its cybersecurity efforts from multiple angles: through the addition of cybersecurity tools and security updates; through staff and agency-wide training; through hiring critical personnel; and through collaboration with OPM's interagency partners. For example, in Fiscal Year 2016, OPM implemented 100 percent multi-factor user authentication for access to OPM's network, via the use of the "Personal Identity Verification" (PIV) card. This capability and enforcement provides a powerful barrier to our networks and information stores from individuals who are not authorized to have access. OPM is in the process of expanding this to agency applications to further increase the security of our systems. In 2016, OPM launched two major IT system compliance initiatives that resulted in all major IT systems having current ATO (Authority to Operate) and network segmentation.

As the Federal government's personnel agency, OPM recognizes that cybersecurity is not just about technology, but is also about people and, to that end, in addition to strengthening its technology, OPM has added seasoned cybersecurity and IT experts to its already talented team. OPM has hired a number of other new senior IT leaders, and realigned and centralized its cybersecurity program and resources under the Chief Information Security Officer (CISO), a primary responsibility of which is to take the steps necessary to secure and control access to sensitive information. OPM also hired Information System Security Officers (ISSOs) in Fiscal Year 2016 to support all of OPM's major information systems.

OPM is continuing to leverage and utilize its interagency partnerships and the expertise of the IT and cyber communities across government. OPM strengthened its threat awareness by enrolling in multiple information and intelligence sharing programs. OPM was one of the first agencies to participate in DHS's Einstein 3A program, and was one of the first agencies in the Federal government to fully implement Phase 1 of DHS's Continuous Diagnostics and Mitigation program. These initiatives allow agencies to detect and prevent cyber-attacks, and continuously identify and proactively mitigate cybersecurity threats and vulnerabilities that might arise.

The cybersecurity incidents at OPM provided an important catalyst for accelerated change across the Federal government. OPM met the challenge and greatly appreciates the collaborative spirit with which its interagency partners across government continue to work with us every day. Embracing modernization can help save taxpayer dollars, improve critical programs, and mitigate security risks in a world of continually evolving threats. OPM and DOD will continue to collaborate on the development of a state-of-the-art IT system for NBIB. By investing in IT systems across functions, we can drive more effective, efficient, and data-driven accomplishment of work across a variety of missions.

Conclusion

The necessary key partnerships and plans have been developed to build out the NBIB and improve the security and efficiency of OPM's IT systems. We created a coordinated strategy to transition the investigative program to an organizational model that fosters innovation, focuses on customer service, and leverages interagency expertise. These structural and process improvements, in coordination with our partners, will enable us to improve timeliness and reduce the investigative backlog. In parallel, we are working closely with DOD's CIO to build the information systems capabilities to support this activity for now and the future. This productive partnership will enable an effective and secure information environment as a government-wide solution. Equally productive is the CIO's holistic approach, which ranges from bringing on new qualified personnel to adopting new tools and procedures that enhance the security of OPM's networks and data for all of OPM's lines of business, including NBIB.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

Thank you for the opportunity to testify before you today, and we welcome any questions you may have.

Kathleen McGettigan

Acting Director of the Office of Personnel Management

Biography

Kathleen McGettigan was named Acting Director of the Office of Personnel Management (OPM) on January 19, 2017. She has an extensive understanding of both the private and public sector, having spent over 25 years dedicated to the Federal service at OPM and 20 years in private sector financial management.

Most recently Ms. McGettigan served as the Chief Management Officer (CMO) at OPM, providing overall organizational insight, analysis and strategic planning to effectively meet programmatic and financial goals of the agency.

Prior to assuming the CMO position, Ms. McGettigan was the Principal Deputy Associate Director for Human Resources Solutions (HRS), which provides reimbursable human resources products and services to meet the needs of the Federal government.

She served as the Deputy Associate Director for the Center for Retirement and Insurance Services from 2003 – 2010 where she was responsible for the provision of retirement and insurance benefits to over 8.5 million customers. During her tenure, she also served as the Chief Financial Officer and Deputy Associate Director for Federal Investigative Services, now the National Background Investigations Bureau (NBIB).

Before entering the Federal sector, Ms. McGettigan was a Senior Accountant at Deloitte, Haskins & Sells and a Vice President and Divisional Controller at Morgan Stanley.
Ms. McGettigan, earned both a Bachelor of Science in Accounting and a Masters of Business Administration in Taxation from St. John's University in New York City. She has been awarded the OPM Director's Award for Distinguished Leadership and the Office of Personnel Management Medal for Meritorious Service, the highest honor bestowed by OPM. She and her husband, Gregory Dean, have two children.

Cord Chase

Chief Information Security Officer

Biography

Cord Chase has accrued more than 18 years of cybersecurity experience, beginning with computer programming, penetration testing, and reverse engineering. Mr. Chase moved up the ranks to serve as the Director of Security Operations and Chief Technology Officer for the USDA. He was quickly recognized as an accomplished Subject Matter Expert in cyber threat intelligence.

Mr. Chase's achievements did not go unnoticed, later serving as the Senior Advisor of Cybersecurity, and a founding member of the Office of Management and Budget's Cyber and National Security Unit. His deep understanding and comprehensive approach was instrumental in the formulation of the highly successful the OMB 2015 30 Day Cyber Sprint.

He was recently appointed as OPM's first official Chief Information Security Officer.

Charles S. Phalen, Jr.

Director of the National Background Investigations Bureau

Biography

Charles S. Phalen, Jr. is the Director of the National Background Investigations Bureau. In this role, he reports to the OPM Director and leads a newly established entity within the U.S. Office of Personnel Management, a government-wide service provider for background investigations. He also partners with the Department of Defense, which is responsible for designing, building, securing, and operating the NBIB information technology systems.

In his previous position, Mr. Phalen was Vice President, Corporate Security for Northrop Grumman Corporation and led the security organization, responsible for overseeing the security policies, procedures and processes that protect company employees, information and property.

Prior to that, Mr. Phalen spent 30 years in the federal service. His most recent government positions include Director of Security for the Central Intelligence Agency (CIA); Assistant Director, Security Division, Federal Bureau of Investigation; Chief, Protective Programs Group, CIA Office of Security; Executive Officer, CIA Office of Security; Center Chief, CIA Office of Facilities and Security Services; and Chief, Facilities and Information Security Division, National Reconnaissance Office. Previously, he worked in or managed security activities involving investigations, operations support, risk analysis, and facility and asset protection, in the United States and abroad.

Mr. Phalen has a bachelor's degree in law enforcement and criminology from the University of Maryland. He is a member of the American Society for Industrial Security and is active in a number of external security forums.

David DeVries
Chief Information Officer

Biography

As the Chief Information Officer, David DeVries serves as the senior digital and information technology advisor to the OPM Director. In this role, in coordination with OPM senior leadership and other stakeholders, he is responsible for defining and implementing a technology strategic vision that aligns with the organization's mission, objectives, and goals. The CIO leads OPM in the adoption of modern, innovative, business and digital solutions, and is the accountable official for all IT and information security operations across the OPM enterprise.

Mr. DeVries joined OPM after serving as the Principal Deputy Chief Information Officer at the Department of Defense.

Mr. DeVries joined the DoD CIO in May 2009 as the Deputy CIO for Information Enterprise, where he was responsible for integrating DoD policies and guidance to create information advantages for department personnel and organizations, and DoD mission partners. Since August 2010, his work has included moving the department towards adopting a Joint Information Enterprise (JIE) based on a single, secure, reliable DoD-wide IT architecture; realizing Secretary of Defense IT efficiencies; creating the way ahead for improved DoD - Veterans Affairs electronic health record exchange capability; expanding cloud adoption and mobile communications capabilities; and establishing key enabling capabilities to achieve the DoD Information Enterprise.

Mr. DeVries has a bachelor of science degree from the United States Military Academy, and a master of science degree in electrical engineering from the University of Washington in Seattle, Washington. He is also a graduate of the Army Senior Service College and served as a Corporate Fellow with IBM Business Consulting Services while participating in the Secretary of Defense Corporate Fellowship Program.

STATEMENT BY

TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

ON

THE NATIONAL BACKGROUND INVESTIGATIONS BUREAU TRANSITON, RELATED INFORMATION TECHNOLOGY SECURITY, AND THE SECURITY CLEARANCE INVESTIGATION PROCESS

FEBRUARY 2, 2017

NOT FOR PUBLICATION UNTIL RELEASED
BY THE HOUSE OVERSIGHT AND
GOVERNMENT REFORM COMMITTEE

Introduction

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for this opportunity to testify before the committee today on the Department's Information Technology (IT) and cybersecurity support to the National Background Investigations Bureau (NBIB). I am Terry Halvorsen, the Department of Defense (DoD) Chief Information Officer (CIO). As the senior civilian advisor to the Secretary of Defense for IT, the DoD CIO is responsible for all matters relating to the DoD information enterprise, including cybersecurity for the Department. In this capacity, the DoD CIO is responsible for oversight of the Department's efforts to design, build, operate, secure, and defend a new IT system to support the background investigative processes for the NBIB. NBIB provides investigative services for more than 100 Federal agencies to make decisions to determine whether individuals meet requirements for new or continued employment; are eligible to hold a sensitive position; or are eligible for access to Federal facilities, automated systems, or classified information. The relationship between DoD and OPM is strong and has been critical to our success thus far on NBIB. David De Vries, OPM's Chief Information Officer, who was previously serving as the Principal Deputy DoD CIO, has helped strengthen that relationship and brings critical IT and cybersecurity expertise to OPM.

As the Department's focal point for the new background investigations IT system, the DoD CIO brings together the Department's full range of IT and cybersecurity resources and expertise. DoD's objective is to replace the current background investigations information systems with a more reliable, flexible, and secure system in support of the NBIB. The Defense Information Systems Agency (DISA), under the DoD CIO's oversight, has established the National Background Investigation System (NBIS) Program Management Office (PMO) to implement this effort. The NBIS PMO is responsible for the design, development, and operation of the IT system capabilities needed to support the NBIB investigative process – to include ensuring cybersecurity protections and resiliency of these capabilities. The alignment of NBIB systems under DoD assures we leverage all national security systems expertise and capability to protect background investigation data.

The Department has made significant headway on this important mission since I previously testified before this Committee last February, and are on track to deliver the capabilities needed in an iterative fashion.

In fiscal year 2016, the Department funded pre-acquisition activities to better posture for official standup and funding in fiscal year 2017. I would like to thank Congress for supporting the Department's funding request for NBIB IT infrastructure and cybersecurity modernization efforts. The fiscal year 2017 continuing resolution (CR) included new start authority for NBIS, which has allowed us to make progress, including awarding a contract last month for the case management prototype. Today, several NBIS prototypes are enabling the Department to work

with industry and discover capabilities that will provide NBIB with a more efficient, effective, secure background investigation IT system in the future. Throughout this process, we are actively partnering with industry and integrating commercial feedback into the process, to ensure that we are focusing on capabilities and keeping up with the changing pace of technology.

Conclusion

I am pleased with the current progress on NBIS that the Department has made to date, and I look forward to seeing what this organization will accomplish as it makes progress toward delivering several prototype capabilities by the end of fiscal year 2017 and initial operating capability covering the full investigative process in the fourth quarter of 2018. This is an important opportunity for the Federal Government to strengthen the security of the IT infrastructure that supports the federal background investigations process. This approach utilizes the Department's recognized IT and cybersecurity expertise, while maintaining a streamlined, centralized, Government-wide approach to the investigations services that NBIB provides today for more than 100 different Federal agencies. I want to thank you for this Committee's continued support for NBIB, and I look forward to your questions.

Terry Halvorsen
Department of Defense Chief Information Officer

Terry Halvorsen assumed the duties as the Department of Defense Chief Information Officer effective March 8, 2015. He previously served as the Acting Department of Defense Chief Information Officer. Prior to that, he was the Department of the Navy Chief Information Officer.

As DoD CIO, Mr. Halvorsen is the principal advisor to the Secretary of Defense for Information Management / Information Technology and Information Assurance as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications. He provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University, and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.