INCORPORATING SOCIAL MEDIA INTO FEDERAL BACKGROUND INVESTIGATIONS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
GOVERNMENT OPERATIONS

AND THE

SUBCOMMITTEE ON
NATIONAL SECURITY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MAY 13, 2016

Serial No. 114–158

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

26–067 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
JACK THORLIN, *Counsel*
WILLIAM MARX, *Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

MARK MEADOWS, North Carolina, *Chairman*

JIM JORDAN, Ohio
TIM WALBERG, Michigan, *Vice Chair*
TREY GOWDY, South Carolina
THOMAS MASSIE, Kentucky
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
GERALD E. CONNOLLY, Virginia, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STACEY E. PLASKETT, Virgin Islands
STEPHEN F. LYNCH, Massachusetts

SUBCOMMITTEE ON NATIONAL SECURITY

RON DESANTIS, Florida, *Chairman*

JOHN L. MICA, Florida
JOHN J. DUNCAN, JR., Tennessee
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma, *Vice Chair*
WILL HURD, Texas
STEPHEN F. LYNCH, Massachusetts, *Ranking Minority Member*
ROBIN KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California

CONTENTS

INCORPORATING SOCIAL MEDIA INTO FEDERAL BACKGROUND INVESTIGATIONS

Friday, May 13, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT OPERATIONS, JOINT
WITH SUBCOMMITTEE ON NATIONAL SECURITY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittees met, pursuant to call, at 9:03 a.m., in Room 2154, Rayburn House Office Building, Hon. Mark Meadows [chairman of the subcommittee] presiding.

Present: Representatives Meadows, DeSantis, Walberg, Jordan, Mica, Hice, Massie, Hurd, Mulvaney, Carter, Grothman, Chaffetz, Connolly, Lynch, Maloney, Lieu, and Kelly.

Mr. MEADOWS. The Subcommittee on Government Operations and the Subcommittee on National Security will come to order. And without objection, the chair is authorized to declare a recess at any time.

We're here today to discuss incorporating social media into the Federal security clearance and background investigations. Having a security clearance means, by definition, you have access to information that would hurt our national security if it got out, and that is why we perform background investigations on individuals who want a security clearance. The goal of our background investigations must be to find out if an individual is trustworthy. Back in the 1950s, that meant talking to neighbors and family.

Today, with more than a billion individuals on Facebook, what a person says and does on social media can often give a better insight on who they really are. Since 2008, various Federal agencies have conducted studies on using social media data in investigations, and they all find the same thing, that there is a wealth of important information on social media.

This issue now facing the Federal Government is how to use social media information while respecting the legitimate privacy concerns that are often brought forth. The good news is that using social media checks in security clearance investigation does not have to be a binary decision between big brother and an ineffective system. There are several reasonable options available to us to use social media data in a responsible way.

It is encouraging to see that ODNI announced this morning, in advance of today's hearing, a new policy that will allow Federal agencies to review publicly available social media information as part of the clearance investigation process. We will continue to

work with the agencies to ensure that the social media data of people with security clearances is used in a safe and responsible way.

Mr. MEADOWS. I would like to thank the witnesses for coming here today and I look forward to their testimony.

And with that, I would recognize the ranking member of the Subcommittee on Government Operations, my good friend, Mr. Connolly.

Mr. CONNOLLY. I thank my friend, the chairman, for holding this hearing to examine the usefulness of social media and other crucial enhancements to the Federal background investigation process.

On January 22, the administration announced that the Federal Investigative Services, a former entity of OPM, would transfer its functions to a new national background investigations bureau. The Department of Defense assumed responsibility for designing and operating all information technology for the new NBIB. I think it makes abundant sense to task our national security experts with protecting the sensitive personal information of millions of clearance holders.

Today, we're discussing another enhancement, the inclusion of social media in the background investigation process. The Army has a pilot program which used publicly available data from social media sites to enhance information available to investigators during background check processes. Currently, the Department of Defense is also conducting a pilot program that looks at all publicly available information online, such as news articles and commercial Web sites. I'm interested in learning the major findings and lessons learned from these pilot programs.

While social media is a promising and valuable source, potentially, of information, I remain concerned that the government should not retain social media data of third parties who happen to engage with the applicant but have not consented to waiving their privacy rights. We must not forget to discuss other ways to enhance security clearance processes.

The Performance Accountability Council is establishing a law enforcement liaison office that will communicate with local governments to expedite the requests for local criminal records. That's a major enhancement. We must remember that on September 16, 2013, Aaron Alexis, a Federal subcontractor with a secret-level clearance, entered the Washington Navy Yard and tragically killed 12 people and injured 4 others. He had a security clearance. The background investigation failed to identify that Mr. Alexis had a history of gun violence. The local police record of Mr. Alexis' 2004 firearms arrest had not been provided to Federal investigators. Improvements in communication between local law enforcement and Federal background investigators could prevent and could perhaps have prevented a tragedy like that that occurred in the Washington Navy Yard.

I welcome each of the witnesses back from the full committee's February hearing and look forward to hearing about their progress on the administration's plan to reform the security clearance and background investigation process, while preserving privacy rights.

Thank you, Mr. Chairman.

Mr. MEADOWS. I thank the gentleman.

The chair now recognizes the chairman of the Subcommittee on National Security, Mr. DeSantis, for his opening statement.

Mr. DESANTIS. Thank you, Chairman Meadows. I just wanted to say, I think this is an important issue. And it looks like that we just got a directive late last night where this is now going to be an implemented policy. So I'm interested in hearing how that's going to be implemented, but I'm sure that's partly as a result of your oversight. So thank you for doing that and I look forward to hearing the witness testimony.

I yield back.

Mr. MEADOWS. Well, Chairman DeSantis, thank you for your leadership on so many of these issues and I look forward to continuing to work with you.

I now recognize the ranking member of the Subcommittee on National Security, the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman. And I would also like to thank Chairman DeSantis and my friend, Mr. Connolly, for holding this hearing. It's important for a number of reasons, which you both have touched on already.

When an individual applies to receive an initial or renewed security clearance, the Federal Government conducts a background investigation to determine whether he or she may be eligible to access classified national security information. Every security clearance candidate is required to complete a Standard Form 86. I have one right here; rather lengthy. It goes into a number of very personal aspects of each person's life. This 127-page form already requests a variety of personal applicant information, such as criminal history, any history of alcohol use or illegal drug use, any mental health counseling. It does not currently request social media information.

But as Chairman DeSantis noted, last night about 11 o'clock, we got copies of this policy. And I want to say thank you. You know, I—we have not always had information forthcoming in a timely manner. Even 11 o'clock at night, that's timely around here, you know, a few hours before the hearing. But I appreciate you sending it.

I thought it might be a mistake, actually, that you sent the policy over. I did have a chance to read it a couple of times last night and it raises some questions, but I think it's a very good first effort. And we appreciate it.

In December of 2015, Congress passed and President Obama signed a bipartisan funding legislation that included a robust directive to enhance the security clearance process. The recent Omnibus Appropriations Act also requires the director of DNI to direct the Federal agencies to use social media and other publicly available government and commercial data when conducting periodic reviews of their security clearance or clearance holders. The law also provides guidance on the types of information that could be obtained from social media and other sources and it may prove relevant to a determination of whether an individual should be granted clearance at all.

Now, this includes information suggesting a change in ideology or ill intent or vulnerability to blackmail in allegiance to another country. The main impetus, as Mr. Connolly noted, was the terrible

situation at the Washington Navy Yard. And also I would add, there has been exploitation of Twitter, Facebook, WhatsApp, and Telegram by the Islamic State. And also at one point we had everyone who filled out a Standard Form 86 hacked by the Chinese as well. So they have a list of everybody who filled out, you know, an 86 requesting security clearance, which is very troubling.

There's a lot that needs to be talked about here. We're going to gather all this information on individuals in one place. In light of what has happened with the Chinese hack, I'm concerned about putting medical information, all of this about people who apply in one place where it might be accessed by hostile or nefarious actors. So we're going to talk a little bit about that this morning.

As I said, I appreciate the Security Executive Agent Directive Number 5 and, you know, I think it's a very good first effort and I appreciate your transparency with us. Thank you.

I yield back.

Mr. MEADOWS. I thank the gentleman. And I will hold the record open for 5 legislative days for any member who would like to submit a written statement.

We'll now recognize our panel of witnesses. I'm pleased to welcome Mr. William Evanina, Director of the National Counterintelligence and Security Center in the Office of the Director of National Intelligence; Ms. Beth Cobert, Acting Director of the U.S. Office of Personnel Management. And I might add, in her new role working incredibly well in a bipartisan and very transparent way that is recognized by this committee. So thank you so much. Mr. Tony Scott, the U.S. Chief Information Officer at the U.S. Office of Management and Budget.

Welcome to you all. And pursuant to committee rules, all witnesses will be sworn in before they testify. So if you would please rise and raise your right hand.

Do you solemnly swear or affirm that the testimony you're about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Please be seated.

Let the record reflect that all witnesses answered in the affirmative. In order to allow time for discussion, please limit your oral testimony to 5 minutes. You're very familiar with the process. But your entire written statement will be made part of the record.

And so, Mr. Evanina, you are now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF WILLIAM EVANINA

Mr. EVANINA. Good morning. Good morning, everyone. Chairman Meadows, Chairman DeSantis, Ranking Member Connolly, Ranking Member Lynch, and members of the subcommittee, thank you for having me here as part of this team to participate in today's hearing.

As the National Counterintelligence executive and the director of the National Counterintelligence Security Center, I'm responsible for leading and supporting the counterintelligence and security activities of the United States Government, which includes the entire U.S. Government and the private sector throughout the intelligence

community. In addition, I'm responsible for providing outreach to U.S. private sector entities who are at risk of becoming a target of intelligence collection, penetration, or attack by foreign and other adversaries.

I also support the Director of National Intelligence's responsibilities as a security executive agent, the role under which the social media directive was developed. And I work close in partnership with the Office of Management and Budget and the Office of Personnel Management, and my colleagues to my left. Department of Defense also partners in this effort as well as part of the PAC. Agencies across the executive branch are also part of today's process and the successes we have achieved with this policy.

When I last appeared before this committee on February 25, we discussed the formation of the National Background Investigations Bureau and security clearance reforms. Today, I've been asked to discuss the administration's policy on the use of social media as part of the personnel security background investigation and adjudication process.

Mr. Chairman, we have been steadfastly at work on a directive that addresses the collection and use of publicly available social media information during the conduct of personal security, background investigations, and adjudications. I want to acknowledge the important contributions to this effort made by our entire executive branch colleagues, particularly at the Office of Management and Budget and OPM. And I'm pleased, as you referenced, to announce that the Director of National Intelligence has recently approved this directive which is being publicly released.

The data gathered via social media will enhance our ability to determine initial and continued eligibility for access to classified national security information and eligibility for sensitive positions.

I realize that the Federal Government's authority to collect and review publicly available social media information in the course of a personnel security background investigation and adjudication raises some important legitimate civil liberties and privacy concerns. Nevertheless, let me be clear. I am strongly of the view that being able to collect and review publicly available social media and other information available to the public is an important and valuable capability to ensure that those individuals with access to our secrets continue to protect them and that the capability can be aligned with appropriate civil liberties and privacy protections.

I would note to the committee that by the term "publicly available social media information," we mean social media information that has been published or broadcast for public consumption, is available on request to the public, is accessible online to the public, is available to the public by subscription or purchase, or is otherwise lawfully accessible to the public.

I believe the new directive on social media strikes this important balance. Under this new directive, only publicly available social media information pertaining to the individual under investigation will be intentionally collected. Absent a national security concern or criminal reporting requirement, information pertaining to the individuals, other than the individual being investigated, will not be investigated or pursued.

In addition, the U.S. Government may not request or require individuals subject to the background investigation to provide passwords or login into private accounts or to take any action that would disclose nonpublicly available social media information. The complexity of these issues has led to a lengthy and thorough review by the departments and agencies that would be affected by this policy, as well as coordination with different members of civil liberties and privacy offices, privacy act offices, and office of general counsel.

Mr. Chairman, the new guidelines approved by the Director of National Intelligence for the collection and use of publicly available social media information and security clearance investigations ensure this valuable avenue investigation can be pursued consistent with subjects' civil liberties and privacy rights.

The use of social media has become an integral and very public part of the fabric of most American's daily lives. It is critical that we use this important source of information to help protect our Nation's security.

Mr. Chairman, I welcome any questions that you and your colleagues have regarding this directive.

[Prepared statement of Mr. Evanina follows:]

Statement for the Record

William R. Evanina

Director of the National Counterintelligence and Security Center

Administration Policy on Use of Social Media for Personnel Security Background Investigations and Adjudications

Hearing before the Subcommittee on Government Operations and Subcommittee on National Security Committee on Oversight and Government Reform United States House of Representatives

May 13, 2016

Chairman Meadows, Chairman DeSantis, Ranking Member Connolly, Ranking Member Lynch, and Members of the Subcommittees, thank you for inviting me to participate in today's hearing.

As the National Counterintelligence Executive and the Director of the National Counterintelligence and Security Center (NCSC), I am responsible for leading and supporting the counterintelligence and security activities of the U.S. Government, including the U.S. Intelligence Community. In addition, I am responsible for providing outreach to U.S. private sector entities who are at risk of becoming a target of intelligence collection, penetration or attack by foreign and other adversaries. I also support the Director of National Intelligence's responsibilities as the Security Executive Agent -- the role under which the social media directive was developed -- and work in close partnership with the Office of Personnel Management (OPM), the Department of Defense, and agencies across the executive branch to govern, enhance, and improve the security clearance process.

When I last appeared before this Committee on February 25th, we discussed the formation of the National Background Investigations Bureau (NBIB) and security clearance reforms. Today, I've been asked to discuss the Administration's policy on the use of social media as part of the personnel security background investigation and adjudication process.

Mr. Chairman, we have been steadfastly at work on a directive that addresses the collection and use of publicly available social media information during the conduct of personnel security background investigations and adjudications. I want to acknowledge the important contributions to this effort

made by our Executive Branch colleagues -- particularly at the Office of Management and Budget (OMB) and OPM. And I am pleased to note that the Director of National Intelligence has recently approved this directive, which is being publicly released. The data gathered via social media will enhance our ability to determine initial or continued eligibility for access to classified national security information and eligibility for sensitive positions.

I realize that the federal government's authority to collect and review publicly available social media information in the course of personnel security background investigations and adjudications raises important and legitimate civil liberties and privacy concerns.

Nevertheless, let me be clear. I am strongly of the view that being able to collect and review publicly available social media and other information available to the public is an important and valuable capability to ensure that those individuals with access to our secrets continue to protect them, and that the capability can be aligned with appropriate privacy and civil liberties protections.

I would note to the Committee that by the term "publicly available social media information" we mean: social media information that has been published or broadcast for public consumption; is available on request to the public; is accessible on-line to the public; is available to the public by subscription or purchase; or is otherwise lawfully accessible to the public. I believe the new directive on social media strikes this important balance. First, under the new directive, only publicly available social media information pertaining to the individual under investigation will be intentionally collected. Absent a national security concern, or criminal reporting requirement, information pertaining to

individuals other than the individual being investigated will not be investigated or pursued. In addition, the U.S. Government may not request or require individuals subject to the background investigation to provide passwords or log into private accounts, or take any action that would disclose non-publicly available social media information.

The complexity of these issues has led to a lengthy and thorough review by the departments and agencies that would be affected by this policy, as well as coordination with different members of Civil Liberties and Privacy Offices, Privacy Act Offices, and Offices of General Counsel.

Mr. Chairman, the new guidelines approved by the Director of National Intelligence for the collection and use of publicly available social media information in security clearance investigations ensure that this valuable avenue of investigation can be pursued consistent with subjects' civil liberties and privacy rights.

The use of social media has become an integral, and very public, part of the fabric of most Americans' daily lives, and it is critical that we use this important source of information to help protect our nation's security.

Mr. Chairman, I welcome any questions you and your colleagues have regarding the new directive.

Mr. MEADOWS. Thank you for your testimony.
Ms. Cobert, you're recognized for 5 minutes.

STATEMENT OF BETH COBERT

Ms. COBERT. Chairman Meadows, Chairman DeSantis, Ranking Members Connolly and Lynch, and members of the subcommittee, thank you for the opportunity to testify before you today on the use of social media in the Federal background investigation process.

OPM plays an important role in conducting background investigations for the vast majority of the Federal Government. Currently, OPM's Federal Investigative Services, FIS, annually conducts approximately 1 million investigations for over 100 Federal agencies, approximately 95 percent of the total background investigations governmentwide. These background investigations include more than 600,000 national security investigations and 400,000 investigations related to suitability, fitness, or credentialing each year.

As we discussed in February, we are in the process of transitioning to the new National Background Investigations Bureau, NBIB, which will absorb FIS and its mission to be the governmentwide service provider for background investigations. The Department of Defense, with its unique national security perspective, will design, build, secure, and operate the NBIB's investigative IT systems in coordination with the NBIB.

To provide some context for our discussion today, I would like to take a few minutes to review how the current security clearance process operates in most cases.

First, an executive branch agency will make a requirements determination as to the sensitivity and risk level of the position. If an agency determines that a position requires a clearance, the employee completes an SF–86 and submits fingerprints, both of which are sent to OPM, along with an investigation request. OPM, through FIS now and NBIB in the future, conducts the investigation by doing all of the checks required by the Federal investigative standards. The results of the investigation are then sent to the requesting agency for adjudication.

The clearance decision is made from the information in the investigative report in conformance with the adjudicative guidelines that are the purview of the Office of the Director of National Intelligence, ODNI.

The requesting agency sends their decision back to OPM, who maintains the records for reciprocity purposes. The individual will also be reinvestigated on a periodic basis.

As the committee is aware, agencies make security clearance decisions using a whole-person approach, meaning that available, reliable information about the person, past and present, favorable and unfavorable, should be considered by adjudicators in reaching a determination.

One component of that approach in the 21st century is the topic of today's hearing, social media. ODNI, in its role as the security executive agent, has developed a social media policy that has undergone extensive coordination with relevant departments and agency officials. OPM looks forward to implementing the policy as part of its ongoing efforts to strengthen its investigative processes.

In April, OPM issued a request for information seeking to better understand the market and the types of products vendors can provide to meet social media requirements. The RFI is in preparation for a pilot that OPM is planning to conduct this year that will incorporate automated searches of publicly available social media into the background investigation process. This planned pilot will be conducted by OPM in coordination with the ODNI.

The pilot will obtain the results of searches of publicly available electronic information, including public posts on social media from a commercial vendor for a population of security clearance investigations using pertinent investigative and adjudicative criteria. This pilot is distinct from other pilots in that it will assess the practical aspects of incorporating social media searches into the operational end-to-end process; the mechanics of adding this type of report to a background investigation and the affects on quality, costs, and timeliness.

In addition, the pilot will assess the uniqueness of the information provided through social media checks as compared to information provided through traditional investigative sources.

Supporting the implementation of the NBIB and aiding its success in all areas will continue to be a core focus for OPM, as well as the Performance Accountability Council, the PAC. Our goal is to have the NBIB's initial operating capability officially established with a new organizational design and leader in place by October 2016. The implementation work will remain to be done after that date.

On behalf of OPM, I am proud to be part of this most recent effort by the administration, and I look forward to working with my colleagues on this panel and with this committee in a bipartisan manner on this important issue. I'm happy to answer any questions you may have.

[Prepared statement of Ms. Cobert follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

TESTIMONY OF
BETH F. COBERT
ACTING DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the
SUBCOMMITTEE ON GOVERNMENT OPERATIONS AND
SUBCOMMITEE ON NATIONAL SECURITY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

"Incorporating Social Media into Federal Background Investigations"

May 13, 2016

Chairman Meadows, Chairman DeSantis, Ranking Members Connolly and Lynch, and Members of the Subcommittees:

Thank you for the opportunity to testify before you today on incorporating data from social media into the federal background investigation process.

NBIB Transition

OPM plays an important role in conducting background investigations for the vast majority of the Federal Government. Currently, OPM's Federal Investigative Services (FIS) annually conducts approximately 1 million investigations for over 100 Federal agencies – approximately 95 percent of the total background investigations government-wide. These background investigations include more than 600,000 national security investigations and 400,000 investigations related to suitability, fitness, or credentialing each year.

As the Administration announced in January, the new National Background Investigations Bureau (NBIB) will be the government-wide service provider for background investigations. The NBIB will absorb FIS and its mission, while adding important new capabilities to improve processes as well as dedicated support in key areas including acquisition and privacy. The Department of Defense (DOD), with its unique national security perspective, will design, build, secure, and operate the NBIB's investigative IT systems in coordination with the NBIB. The NBIB leadership will be headquartered in Washington, D.C., which will facilitate smooth and efficient coordination with interagency partners.

Testimony of Beth F. Cobert
U.S. Office of Personnel Management

May 13, 2016

Since my appearance before this Committee in February to discuss the implementation of the NBIB, we now have in place a transition team to oversee and manage this transition. The team is composed of senior government officials, many of whom come from Performance Accountability Council (PAC) member agencies. These individuals have brought expertise in the background investigations and security clearance processes as well as crucial experience in leading government organizations through complex transitions. The team has hit the ground running and is making progress laying the foundation for this transition.

Social Media and Federal Background Investigations

As the Committee is aware, agencies make security clearance decisions using a "whole person" approach, meaning that available, reliable information about the person, past and present, favorable and unfavorable, should be considered by adjudicators in reaching a determination. Background investigations provide agency adjudicators with the information needed in each case to examine a sufficient period of a person's life to make an affirmative decision that a person is an acceptable security risk.

One component of that approach in the 21st century is the topic of today's hearing – social media. The Office of the Director National Intelligence (ODNI) in its role as the Security Executive Agent has developed a social media policy that has undergone extensive coordination with relevant department and agency officials, including the agencies with significant national security missions and the Federal CIO Privacy Committee. ODNI has taken a deliberative approach in developing its policy. It was informed by social media pilots conducted by multiple agencies, including DOD, giving insight into the issues, costs, and benefits associated with conducting a social media check as part of the personnel security vetting process. Continued analysis of the results of the pilots will guide the way forward and identify areas requiring additional research. This policy is being finalized and, once signed by the ODNI, will be issued. OPM, through the NBIB, looks forward to implementing the policy and guidance to strengthen its investigative processes.

OPM's Request for Information and Pilot Project

In April, OPM issued a Request for Information (RFI) seeking to better understand the market and the types of products vendors can provide to meet social media requirements. The RFI is being conducted in preparation for a pilot OPM is planning to conduct that will incorporate automated searches of publicly available social media into the background investigation process. This planned pilot project will be conducted by OPM in coordination with the ODNI to obtain the results of searches of publicly available electronic information, including public posts on social media, from a commercial vendor for a population of security clearance investigations using pertinent investigative and adjudicative criteria. This pilot is unique from other pilots in that it will assess the practical aspects of incorporating social media searches into the operational end-to-end process; the mechanics of adding this type of report to a background investigation; and the effects on quality, costs and timeliness. In addition, the pilot will assess the exclusivity of information provided through social media checks as compared to information provided through traditional investigative sources.

Testimony of Beth F. Cobert
U.S. Office of Personnel Management

May 13, 2016

Conclusion

Supporting the implementation of the NBIB and aiding its success in all areas will continue to be a core focus for the OPM as well as the PAC. I know that the PAC will monitor the NBIB's performance in order to identify, propose, and help drive enterprise-level process enhancements. The PAC will make recommendations for changes to Executive Branch-wide guidance and authorities and will also develop, implement, and continuously re-evaluate and revise outcome-based metrics that help measure the effectiveness of the vetting processes, including the use and benefits of social media.

Our goal is to have the NBIB's initial operating capability officially established with a new organizational design and leader by October 2016, though implementation work will remain to be done after this date.

On behalf of OPM, I am proud to be a part of this most recent effort by the Administration, and I look forward to working with my colleagues on this panel and with this Congress in a bipartisan manner on this important issue. I am happy to answer any questions you may have.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
1900 E STREET NW, WASHINGTON, DC 20415

Over the course of her career, she led McKinsey's initiatives on recruitment, training, development, performance evaluation, and retirement services and championed efforts to support the advancement of women into leadership positions.

Cobert also previously served as a board member and chair of the United Way of the Bay Area and as a member of the Stanford Graduate School of Business Advisory Council. Cobert received a bachelor's degree in economics from Princeton University and a master's degree in business administration from Stanford University. She and her husband, Adam Cioth, have two children.

Mr. MEADOWS. Thank you for your testimony.
Mr. Scott, you're recognized for 5 minutes.

STATEMENT OF TONY SCOTT

Mr. SCOTT. Thank you.
Chairman Meadows, Chairman DeSantis, Ranking Member Connolly, Ranking Member Lynch, and members of the subcommittees, I appreciate the opportunity to appear before you today.

The administration recognizes the importance of gathering accurate up-to-date and relevant information in its background investigations to determine Federal employment and security clearance eligibility. And as a government, we must continue to improve and modernize the methods by which we obtain relevant information for these background investigations.

Since 2009, various government agencies have conducted pilots and studies of the feasibility, effectiveness, and efficiency of collecting publicly available electronic information as a part of the background investigations process. Those pilots have informed the development of a new social media policy that has been issued by the director of National Intelligence in his role as the security executive agent. And I will defer to ODNI on the further details of this policy.

But as you know, OMB chairs the interagency Security and Suitability Performance Accountability Council, or PAC, to ensure interagency coordination. And the new policy will reflect, I believe, an appropriate balance of a number of considerations, such as protecting national security; ensuring the privacy of and fairness to individuals seeking security clearances and associates of that individual; the veracity of the information collected from social media; and the resources required to process the collection, adjudication, and retention of the relevant data collected.

As the policy is implemented, the administration will continue to assess the effectiveness and efficiency of the policy. To do so, the government must keep pace with advancements in technology to anticipate, detect, and counter external and internal threats to the Federal Government's personnel, property, and information. This need must also be considered with the full legal and national security implications in mind. I'm confident that this new policy will strike the correct balance between all of these considerations.

I thank the committee for holding this hearing and for your commitment to improving this process. We look forward to working with Congress, and I'm pleased to answer any questions you may have.

[Prepared statement of Mr. Scott follows:]

Embargoed until Delivered

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/omb

TESTIMONY OF TONY SCOTT

UNITED STATES CHIEF INFORMATION OFFICER
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEES ON GOVERNMENT OPERATIONS AND NATIONAL SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

May 13, 2016

Chairman Meadows, Ranking Member Connolly, Chairman DeSantis, Ranking Member Lynch, and Members of the Subcommittees, I appreciate the opportunity to appear before you today to speak about the important issue of incorporating social media in the Federal government's background investigation process.

Use of Social Media in Background Investigations

The Administration recognizes the importance of gathering accurate, up-to-date, and relevant information in its background investigations. That information is necessary to make important decisions about eligibility for Federal or contractor employment and a security clearance.

As technology evolves and our economy becomes more digitally connected, we are cognizant that the sources from whom we obtain relevant information must change over time and that the government must constantly seek to improve its background investigation methods and processes to leverage those advances.

What the Administration Has Done

Since 2009, various government agencies – including the Department of Defense and elements of the Intelligence Community – have conducted pilots and studies of the feasibility, effectiveness, and efficiency of collecting publicly available social media information as part of the background investigations process. Those pilots have informed the development of a new social media policy that will be issued by the Director of National Intelligence in his role as the Security Executive Agent.

And as you know, OMB chairs the interagency Security and Suitability Performance Accountability Council or "PAC" to ensure there is coordination on such reforms. The policy will reflect, I believe, an appropriate balance of a number of considerations, such as:

- protecting national security;
- the privacy of, and fairness to, the individuals seeking security clearances *and* associates of that individual;
- the veracity of the information collected from social media, and whether social media information was unique, or had already been collected from existing sources; and
- the capacity of and the cost to agencies and the security clearance process to accommodate collecting and adjudicating relevant information.

I will defer on the details to the Office of the Director of National Intelligence (ODNI) as the Security Executive Agent issuing the policy. As it is implemented, the Administration will continue to assess the effectiveness and efficiency of the policy.

Conclusion

There is no question that we must keep pace with technological advancements to anticipate, detect, and counter external and internal threats to the federal government's personnel, property and information. This need must also be considered with the full legal and national security implications. I am confident that the policy the Security Executive Agent is about to issue will strike the correct balance between all these considerations. I thank the Committee for holding this hearing, and for your commitment to improving this process. We look forward to working with Congress and I am pleased to answer any questions you may have.

Mr. DESANTIS. [Presiding.] I thank the gentleman.

The chair now recognizes himself for 5 minutes.

And this is for each of you. Are your agencies utilizing commercially available software to vet security clearance applicants, monitor security clearance holders, and detect any cybertheft of these individuals' personal information?

Ms. COBERT. Congressman, in the process of the investigations, we do work with commercial vendors of publicly available vetted information. That is sort of our core element. We use that and other methods to gather the information in the investigative process. I'm not sure if I've completely answered your question.

Mr. DESANTIS. Well, there's certain off-the-shelf technology that the Federal Government will use in other instances, and I just wanted to ask if there is any type of prohibition on doing that or if you guys just aren't doing that or you're actually trying to using all the tools that are potentially at your disposal?

Ms. COBERT. We use a variety of tools to gather information from public sources, from both governmental and nongovernmental, so there's a variety of tools we use to do that. Those are used to, you know, gather some of the information, whether there's a national, you know, law enforcement database from which we get information. We do, for example, use electronic methods to gather appropriate—appropriately gather information about financial history. So we do use some of those tools. I'd be happy to get back to you with more of the specifics, if that would be helpful.

Mr. DESANTIS. Okay. Thank you.

Mr. EVANINA. Sir, I would concur with my colleague. I think we encourage the most robust and effective, efficient tools that are processed for ensuring a speedy, effective background investigation. That's going to be different—this process will be different, depending which agency is doing the background investigation, the tools that they are capable of, the expense, and the number of—the volume of people that are applying for a clearance.

Obviously, we would encourage the ODNI, the most effective and efficient off-the-shelf capabilities, as long as it's within the rules, regulations, and policies set forth.

Mr. DESANTIS. Let me ask you this: In the years leading up to Edward Snowden's theft of classified info, he made several posts to online forums using a consistent user name complaining about government surveillance. And these posts may have alerted authorities that he could be an insider threat. Have any of the social media pilot programs evaluated to date been capable of detecting that sort of post where the subject is posting under an online identity that is not explicitly the individual's name?

Mr. EVANINA. Sir, I'm not specific to the exact nature of the depth and granularity of those particular pilots. But I can tell you, those particular posts from Mr. Snowden that he did would not have been caught in the social media because it's not public facing and there was private chats with other individuals beyond the password protection.

Mr. DESANTIS. So if they're using semi-anonymous names, to the extent that there are public forums, would requiring the disclosure of any alternative online identities on the FS–86 form be something that would be helpful?

Mr. EVANINA. Sir, we're currently not planning on asking anyone to provide any other alternative passwords or email accounts or individual reference to their online persona.

Mr. DESANTIS. So, basically, if—so we'll look at social media, if they're posting. If John Smith applies for security clearance and you'll look for John Smith, but if he goes by, you know, Jack Scott, then you're just not going to require that. So they can post whatever there and that's not going to be something that would be considered?

Mr. EVANINA. Not currently, unless they're willing to consent to provide that information to us.

Mr. DESANTIS. Okay. What reason could allow extensive questioning of friends—so I mean, the FS–86 is a very intensive investigation. I mean, you'll call up people's college roommates. You'll call up people's neighbors when they've lived—even if they've lived in a place for a short period of time. So there's a lot of extensive investigation. So why would you want to do that? And I'm not saying you shouldn't do that, but why would you want to do that but then not get the whole, I guess, picture of their online identities?

Mr. EVANINA. Well, I think if the additional information is obtained that an individual has a pseudonym or has—an individual has an offline persona that's different than his name, that can be pursued investigatively, but that's not something we are going to ask, or there's really not a way for us to identify Bob Smith who is really Dave Jones online without someone telling us that.

Mr. DESANTIS. But what would be the reason to just—since there's so much information required in the FS–86, what would be the negative of just asking, hey, do you post online under any type of pseudonym?

Mr. EVANINA. I think when you get past the public-facing interface of social media, you get to the, I think, the border of privacy and civil liberties in terms of what are your practices beyond what you would do in the course of your daily lives. And by this, the analogy would be, we don't look at their emails and we don't look at their telephone conversations as part of the background investigation as well.

Mr. DESANTIS. Okay. My time is up.

I now recognize the gentleman from Virginia for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman, and welcome.

Help me understand how this works. Because it's one thing for a private individual to be sort of trolling in Facebook; it's another for the government to be doing it. And so how does this work? I mean, I—somebody in government gets on the Internet and looks up your Facebook history? You're subject—you're Harry Houdini. You've applied for a security clearance and we're looking at, you know, through social media, anything that you used, Twitter, Facebook, YouTube, Hulu, whatever it might be. So we just go online and look at whatever we can find under his, Harry Houdini or Shirley Jones' name. Is that right?

Mr. EVANINA. Sir, I'll start—I think——

Mr. CONNOLLY. If you could pull the mic closer. Thank you.

Mr. EVANINA. I'm sorry, sir.

Congressman, I think when we set forth this policy, we looked at it and tried to provide the most flexibility for investigative agen-

cies and service providers to do what they feel is most practicable and most reasonable for their individual agency. So, for instance, some of the bigger agencies may provide a data service provider, they aggregate this data for multiple people to go out and do the search. We are clearly acknowledging that the effort will be exhaustive initially to identify people's social media footprint that's out there.

Mr. CONNOLLY. Okay. What are the red lights, though, that flag for us, got to follow up on this? So, you know, my Facebook posting, you know, we're talking about the block party for July in my culde-sac. You know, talking about maybe a family reunion and interspersed with all of that, oh, by the way, the President needs to die. How do we flag the serious from the trivial and how do we make sure that if it's all trivial, that's the end of it. It's deleted, it's not retained, because there may be other names in that Facebook. There may be pictures of other people who are not the subject of an investigation, unless that association is suspect.

How do we make sure that we don't just have some enormous government depository of personal information of American citizens that's really not at all relevant, or parts of it may be? How do we do that?

Mr. EVANINA. That's a great question, Congressman. I think, putting this in context, the social media utilization is just one tool of many that we currently already use in background investigations. And the collection and retention of that data will be parallel to any other data we collect on an individual. And to your example of Facebook, and the examples you gave, the only relevant information that were there for investigative adjudicative processes would be the issue to the President. All the other stuff would not be retained, although we would collect and retain the Presidential, if——

Mr. CONNOLLY. Let me interrupt, though.

Mr. EVANINA. Yes, sir.

Mr. CONNOLLY. God forbid, but should there be such a reference, well, the other stuff is not being retained. Actually, I might now want to take a fresh look at your associations because maybe they're involved or—I mean, wouldn't we want to check that out?

Mr. EVANINA. Sir, so I was going to say——

Mr. CONNOLLY. If for no other reason than to talk to the neighbors to say, does Harry Houdini talk this way often? Have you ever heard him—you know, right?

Mr. EVANINA. Right. So the social media application here, like many other tools that are at the disposal of investigators, would provide an investigative lead. So that particular post on your Web site would lead to an investigative lead to be furthered up with your colleagues, your family, your friends, your neighbors as just another lead; no different than we would find in an anomalous financial disclosure.

Mr. CONNOLLY. Ms. Cobert and Mr. Scott, in the time I have left, I'd be derelict on behalf of my constituents if I didn't return to the OPM security breach, and if you can take some time to bring us up to date. Weaknesses identified, have they been addressed so that there can't be a recurrence? And how are we coming in trying

to make people whole again in terms of the compromise of their personal information?

Ms. COBERT. Let me start in the response to that one. In terms of improving the security of our systems, we have made significant strides in our ongoing effort and we will continue to do so. Working closely with DHS, with DOD as part of the NBIB standup, we actually have staff from DOD now on site working with us as well as ongoing working sessions. We've installed the latest versions of EINSTEIN. We've got a whole series of improvements that we've made to our firewalls. We now have the ability to much——

Mr. CONNOLLY. Excuse me, EINSTEIN 3 is in place now?

Ms. COBERT. We are one of the first agencies to put that in place.

Mr. CONNOLLY. Because it wasn't in place at the time of the breach, right?

Ms. COBERT. No.

Mr. CONNOLLY. Right. Excuse me.

Ms. COBERT. So we continue to work to try and put in place a whole series of tools and we've seen real improvements in that, as well as strengthening. We have a new chief information security officer. I could go on and on, but we still will continue to work at that issue.

In terms of the individuals whose information was taken, we have the identity theft, identity monitoring contracts in place. We continue to monitor those in terms of the quality of their customer service. We are also actively working to put in place the provisions to extend the identity theft insurance to $5 million, as well as being in the process of figuring out how to extend those to the 10 years that was also approved by Congress. So we continue to work at these quite closely, including with Tony and the team from OMB.

Mr. SCOTT. And I would just add, I'm seeing almost as much of Beth as I did when she was at OMB as we work on this project. And Beth and I and the DOD CIO meet regularly to review the progress that the teams are making in both the transition, but also ensuring the security and integrity of the existing system. So I'm pleased with the progress.

Mr. CONNOLLY. Thank you.

Thank you, Mr. Chairman.

Mr. DESANTIS. The chair now recognizes the gentleman from Georgia, Mr. Hice, for 5 minutes.

Mr. HICE. Thank you, Mr. Chairman.

Mr. Evanina, let me begin with you. As we all know, in 2008, there was a commissioned study in regard to showing the benefits of examining certain aspects of social media. Why has it taken 8 years to implement this thing, to get it started?

Mr. EVANINA. Congressman, I can't really answer the 8-year issue, but I can tell you that to get to where we are took a lot of extensive effort and interagency coordination to be able to strike the right balance between what we need to obtain or should be obtained reasonably from social media in the ever-growing Internet age and balance that with the civil liberties and privacy of our, not only clearance holders, but U.S. citizens. So that process not only was exhaustive, but it was the right thing to do.

Also, I think with the pilots that have started and continue to move on, we haven't really identified the correct value or weighted measure for what the efforts of social media collection will be or has been. So we're still efforting the pilot process to identify, is the effort resource allocation worthy of collecting other social media and using it as part of the background investigation process, number one. And number two, if it is, where do we allocate that within the investigative process, the beginning, the middle, the end? Because it will be resource intensive.

Mr. HICE. Well, it seems like 8 years is an awfully long time to try to find a balance between privacy and, you know, that which is public information. I mean, this is not highly private information that people are publicizing out on social media like this, and I understand that we want to be very careful with that. We all do. But——

Well, let me ask you this: It seems that the new policy that we saw this morning, that within there—and correct me if I'm wrong, but it seems like finding information on an individual's background appears to be largely at the discretion of individual agencies. Can you tell me why ODNI decided to leave that decision to individual agencies rather than opening this up for all departments of our Federal Government?

Mr. EVANINA. That's a great question, Congressman, but I will say that there's only 22 agencies who have the authority to conduct background investigations. So—and they do that on behest of all the other Federal organizations or agencies' departments who require that. So those individuals, the ones who are covered under this policy, the policy was purposely made flexible because I will proffer that from 2008 till 2 years ago, the social media definition has changed dramatically and will continue to change.

So in order to provide the agencies who conducted the investigations the maximum flexibility to go about utilizing social media as part of this process was paramount in this effort. Because I'm pretty sure a year from now, the social media definition may change, and we wanted to make sure that each agency had the flexibility, from a resource perspective, to identify the best, most efficient way to implement this policy.

Mr. HICE. Do you believe those other 22 agencies will begin utilizing this?

Mr. EVANINA. I do.

Mr. HICE. Okay.

Ms. Cobert, could you explain how OPM plans to implement this policy?

Ms. COBERT. Thank you, Congressman. As I mentioned in my testimony, we are working through this pilot process to figure out the best way to utilize social media as a standard, consistent part of the process. As Mr. Evanina described, we are committed to its value. It's a question of how.

We need a way to make sure that when we gather information on social media, it's accurate. It's is not always accurate. What you find is not always the reality. We need to find a way to make sure, as we do this, that we have the resources to follow up on whatever information is revealed. How do we get those resources to follow up on those things?

And so that is the goal of this pilot, is to embed it into the operational process. Are there places where, by using social media or other tools, we can replace some steps that exist today, take those resources and deploy them to something else? Are there other cases where the value of the information will merit adding additional resources? So that is the issue we're working through.

And the pilot process that we are starting, we'll be starting that pilot before the end of this fiscal year. We also will continue, through the PAC and other forums, working with DOD and other agencies as they start to implement this so we all can learn from each other. We've got to figure out how to do this right and to do it at scale, and we want to move expeditiously but cautiously as we do that.

Mr. HICE. Thank you. Could you provide the committee with a timeframe for implementation, besides just by the end of the year, a more specific timeframe?

Ms. COBERT. We'll get back to you. The first piece is the pilot and then we will take that learning. But we're happy to provide you some more information on what we're doing next.

Mr. HICE. Okay. Thank you very much.

I yield back.

Mr. DESANTIS. The gentleman's time has expired. The chair now recognizes Mr. Lynch from Massachusetts for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. And I want to thank everybody for holding this hearing and thank the witnesses for their help.

You know, every once in a while, my happy talk alarm goes off and sometimes I think I'm hearing happy talk and I think I just heard some.

Look, I appreciate the idea that, you know, we got this 8-year continuum of improvement and we're trying to improve our systems and, you know, there's this cautious progress of protecting and balancing, you know, private information, versus, you know, doing these background checks. But the reality on this committee is 10 months ago, Ms. Cobert, your predecessor, Ms. Archuleta, sat there and told me that, 10 months ago, we were not even encrypting the Social Security numbers of the 4 million people who were hacked at OPM. That's the reality. Ten months ago we weren't even encrypting Social Security numbers. And she painfully had to admit that, and her legal counsel was with her and they confirmed that fact.

So I'm very concerned about what is happening. And I am very encouraged that DOD is going to take over cybersecurity in your shop and you're going to help them with that. How is that going? And what steps have you taken—be specific—that should give me some level of reassurance that we don't have another problem like that?

Ms. COBERT. Thank you, Congressman. Let me start with how we're working with DOD in the standup of the NBIB, and then I can come back to some things we have underway and that we will be doing in that context.

We are working very closely with DOD, as Mr. Scott described, in a process to do two things.

Mr. LYNCH. Let me just cut you off because I don't want to go into this long diatribe. But have you encrypted the Social Security numbers for all of the employees right now at OPM?

Ms. COBERT. There are still elements of the OPM systems that are difficult to encrypt. We have a multilayer defense.

Mr. LYNCH. And you've got all of these different systems and I understand that. I'be been at this a while, okay, and we have tried to get ahold of this. And I've been here for years working on this problem and it's been very difficult. And there's no shame in admitting how difficult that is. What I don't want is happy talk that it's all going well. That's the problem. Because then we'll have another hearing and, you know, there will be a lot of gnashing of teeth and criticisms, you know, and there will be somebody else in your spot.

So what I'm trying to get at is, what are we actually—what are we getting done and where are the obstacles? If there are obstacles here in terms of what you're trying to do—and I believe you're all trying to do the right thing. Mr. Scott as well. You can get in on this because you're part of this.

You know, what are we actually doing to try to protect the information that we do gather?

Mr. SCOTT. Well, I would say, as Beth was saying, there's been all kinds of work done in this area, penetration testing, new tools deployed, multiple examinations, and ongoing help from DOD, DHS, and so on. So I think OPM actually is leading Federal agencies right now in terms of, you know, their efforts and the amount of progress that they've made. They've applied tools to the limits that they can within the limits of current technology. But as Beth said, there's some things that just can't be encrypted because the technology doesn't allow it.

Mr. LYNCH. DOD's funding in this area is much better than OPM's and some of the other departments. And so are we using their personnel now? Have they come over and taken over this?

Mr. SCOTT. Absolutely. They've been in there side by side with the team at OPM helping not only review, but look at architecture and also build out the plans for the future NBIB technology. So I'm pleased with where it's going. I don't think there's anybody who would say our job is done or that we're not, you know, interested in pursuing what else we can do.

Mr. LYNCH. The cost estimate, you know, we've had some pilot programs that tell us it's somewhere between, you know, $100 and $500 per person for a private vendor to do these screenings, this gathering of social media information. Is that pretty close to what the—in practice what we're finding?

Mr. SCOTT. Yeah, I would say some of the pilots that have run, the estimates have been in that range. Clearly, one of the things that will have to happen, and I think the pilots will inform this, is some greater level of automation. As you can probably appreciate, when you do a search, you get a ton of data that has to be sifted through and adjudicated.

Mr. LYNCH. Right.

Mr. SCOTT. And I happen to be a person who has a name that's shared with, you know, a professional baseball player, a professional musician, a movie director, and a bunch of other things, and

just a simple search would turn up a bunch of crazy stuff that wouldn't be relevant.

Mr. LYNCH. Yeah.

Mr. SCOTT. So some degree of automation, ultimately, is going to have to help bring the cost down of that.

Mr. LYNCH. All right. I see my time has expired.

Mr. Chairman, thank you for your indulgence, and I yield back.

Mr. MEADOWS. [Presiding.] I thank the gentleman.

The chair recognizes the gentleman from Kentucky, Mr. Massie, for 5 minutes.

Mr. MASSIE. Thank you, Mr. Chairman. This is a great hearing. Thank you for conducting it.

I have a friend who suggests that the government should outsource this background research to the consultants that do opposition research on us, on the politicians, because they seem to find anything all the way back to junior high. But on a serious note, though, you know, I see Edward Snowden as an example here in our notes as somebody who maybe you would have known something about if you had done social media research. That may or may not be true.

But one thing that does stand out is that political contributions are available online and they—and I suppose even before social media and the online availability of this, they were available. So you already have an analog or probably a way of considering whether you should consider or not consider political contributions when doing background research.

But now that you have social media available to you, there's another layer of transparency—or layer of opaqueness that has been removed. You can see where somebody supports a political candidate or not. By the way, Edward Snowden and I have similar contribution histories so—and my colleague here suggested that you should be suspect of anybody that contributes to me as well.

But my question is this: Do you, Mr. Evanina, do you take into account political support when you're doing background research in social media?

Mr. EVANINA. We do not. I mean, I think it's important for the committee to understand that the investigators who conduct the background investigations are very well trained and they follow the Federal investigative standards. And there are plenty of policies that they put forth in their rigorous background investigation and they conduct investigations on information obtained that's relevant to whether or not you're capable of obtaining and holding a security clearance. So a political contribution would not be one of those.

Mr. MASSIE. So if they encountered somebody who in their social media supported a candidate who was strong on the Fourth Amendment and believed very strongly in the right to privacy—and there are different interpretations of the Fourth Amendment. I'm not saying everybody doesn't believe strongly in the Fourth Amendment—that wouldn't be a consideration?

Mr. EVANINA. Absolutely not. Whether you believe in the Fourth Amendment would not have any predication on whether you could hold or maintain a security clearance.

Mr. MASSIE. Thank you very much.

And I will yield back my time.

Mr. MEADOWS. I thank the gentleman.

The chair recognizes the gentlewoman from Illinois, Ms. Kelly, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair.

Many of us have become so accustomed to using technology in our day-to-day lives that it seems second nature to examine the social media accounts of individuals applying for security clearance. However, it's important to note that when incorporating social media into the Federal background check process, a number of steps must be taken that go far beyond those we view as a friend's Facebook profile.

Ms. Cobert, OPM conducts approximately 95 percent of background checks governmentwide. That's in our notes. The initial data collection portion of these investigations is completed by Federal contractors, in part, because you must comply with the various laws governing what information can be collected, used, and stored by the Federal Government. Is that accurate?

Ms. COBERT. Congresswoman, we work with Federal contractors in the investigative process to enhance our capacity to conduct background investigations. They have to follow the same Federal investigative standards that Mr. Evanina referenced. There, the individuals from those contractors who work on investigations also have to undergo thorough training against those standards, and we work to ensure that that is the appropriate training.

Ms. KELLY. Okay. The incorporation of social media data is not as simple as it may sound to many people, so I'd like to delve a little deeper into how we get from a vendor running query for publicly available information to the point at which we have valuable verified information for use in the adjudication process. Again, to begin with, contractors must conduct social media checks on clearance applicants based on guidance from you about the kind of information relevant to clearance investigations. Correct?

Ms. COBERT. We are going to start with the social media thing, the social media efforts with the pilot I mentioned. That will help us understand what kind of guidance we should be putting in place when individuals are conducting social media searches to verify that information, to ensure we're focused on the pieces that are relevant to a security clearance, not the other issues that are not part of the process. That's why we're going to work this through in a pilot so we can create standards and processes that will get us relevant information, reliable information, and protect privacy.

Ms. KELLY. And then your current contractors will need proper training and proper guidance to do all of that.

Ms. COBERT. They will need training. Yes, they will.

Ms. KELLY. Once the data has been collected, a human being is necessary to make a judgment and verify that it does, in fact, belong to the individual in question.

Ms. COBERT. We are working to find the processes that will enable us to, in fact, match individuals. As Mr. Scott described, there are multiple Tony Scotts. So we are working through the pilots, and I think this will be an ongoing process, to see where are the places where we need human intervention; where are the places where technology can help with that resolution?

Ms. KELLY. Okay. Mr. Evanina, can you speak to some of the challenges associated with verifying identities in social media data?

Mr. EVANINA. Yes, Congresswoman. I think the challenges cannot be understated in where we're headed in terms of, number one, identity resolution. As my colleagues have mentioned, the ability to identify Bob from—or Mr. Scott from Mr. Scott and all that goes with it, the resources that it will take to make sure that we are firmly in agreement that Mr. Scott is Mr. Scott. Then, what we found out on Mr. Scott, is it investigatively and adjudicatively relevant? Does it make sense to put forward? And if it is, then it gets put in the same box all other investigative data would be to make sure that it follows the policies, procedures, and the investigative standards and guidelines.

I want to reiterate that social media identification of information is in the same box of all other tools and techniques investigators have.

Ms. KELLY. And even after we have verified an individual's account, additional manual processing is needed in order to analyze, interpret, and contextualize information, particularly photographs. Is there any way to fully automate the analysis of photographs?

Mr. EVANINA. Well, I want to refer back to my colleague, Ms. Cobert, in terms of the ability to maximize any type of automation we can to facilitate not only the effectiveness of this tool, but at the end of the game. But I want to inform the committee that at the end of the day, no matter what we identify, the adjudicator is a fundamentally government role. So the adjudicator will make the ultimate decision if the individual is Mr. Scott, the information pertaining to him is investigatively relevant, and it should be a value-add to whether or not he gets a clearance or not.

Ms. KELLY. Okay. Thank you.

I yield back the balance of my time.

Mr. MEADOWS. Thank you.

The chair recognizes the gentleman from South Carolina, Mr. Mulvaney, for 5 minutes.

Mr. MULVANEY. I thank the chairman for the opportunity. Thank you all for coming. I've just got a couple sort of random questions.

Mr. Evanina, you said something during your opening statement I want to go back to, which is you—and a couple of you used the same terminology and maybe I just don't understand the issue. And full disclosure. Mr. Massie and I are sort of in the libertarian-leaning wing of the party, so we take civil liberties very seriously. And you mentioned that there were civil liberties concerns, I think, in doing this research in the first place. I don't get that.

What civil liberty of mine could be at risk from you doing research on me?

Mr. EVANINA. Well, I—correct. I don't think in terms of the previous pilots and this particular policy——

Mr. MULVANEY. Right.

Mr. EVANINA. —in order to get to where we were, we had to negotiate strongly to ensure that each individual who applies for a security clearance, we are going to protect their privacy and civil liberties, at the same time collect the information that we deem necessary to ensure they can get a clearance.

Mr. MULVANEY. And, again, I'm not trying to split hairs with you, but if I'm coming to you—and we've had this—a very similar discussion, Mr. Chairman, when it comes to folks who want to come into the country on various visas. The lady who shot the people in San Bernardino came on a fiance visa, and we didn't do any social media on her. And one of the arguments we got from customs enforcement was that it would violate her civil liberties to go and do that. Okay?

If I come to you and I'm asking for a job, or I'm asking in my current job to get a security clearance, can't you just get my permission to go look at everything?

Mr. EVANINA. Yes, sir. As a matter of fact, when you apply on an SF–86, the very first thing you get to do is consent to the government searching you, not only with regard to social media, but all your other financial, medical records, you consent to do that on the SF–86.

Mr. MULVANEY. Okay. So there's no privacy concerns. Because I have the right to waive that and I do. Right?

Mr. EVANINA. That's correct.

Mr. MULVANEY. So there's absolutely no privacy issue on the front end when you're doing your background research on me, correct?

Mr. EVANINA. As long you consent to it——

Mr. MULVANEY. Right.

Mr. EVANINA. —on your SF–86.

Mr. MULVANEY. Okay. Good. Good. Then we're all on the same page. Because then the real privacy concerns comes with what Mr. Lynch mentioned, which is what do you do with the information on me after you have it? Because while I consent to let you go and get it, I certainly don't consent with you giving it to other people.

So I think that's why the focus, I think, for many of us who are interested in our civil liberties there is what are you doing after you have it. And I want to go a little bit deeper than just the Social Security numbers, because I think Mr. Lynch properly pointed out, what are you doing with Mr. Massie's medical records when you're doing the research on him? How are we——

Mr. CONNOLLY. Massie.

Mr. MULVANEY. Yeah, especially on Massie, right? And his mental health records. No.

Mr. CONNOLLY. Actually, I've got it right here. Page 17 is kind of interesting.

Mr. MULVANEY. So tell me about that. Because, again, we all know about the risks. Everyone in the country now has gotten a hard wire to sort of think, well, my Social Security thing is really important. I hope they're protecting that. But what about the stuff that doesn't, on its face, look like it could be damaging to us?

You know, maybe Mr. Scott went to marriage counseling. Okay. Not illegal. And I don't even know if that's true, and I am not even suggesting it is. I am using it as an example. It's not illegal. It's certainly not the type of thing, though, that you want to have public. What are you doing to protect that kind of information? Not just the number data, not just the Social Security numbers, but the detail, the meat of the stuff that you might find on anybody that you're looking at.

Mr. EVANINA. I'll start and pass to my colleague, but I want to ensure that the only collection and retention of data will be what is investigatively relevant to completing and authorizing a background investigation. If it's not relevant to you obtaining a clearance, it won't be retained.

Mr. MULVANEY. Okay. Let's focus on that one word then, because again, that's an open-ended questions that I've asked. Let's narrow it down.

Nothing is not retained anymore. Okay. Once you have it, it's some place. Even if you hit erase on your hard drive, it's some place. So what are you doing to make sure the stuff that you don't retain really isn't retained?

Ms. COBERT. Congressman, when we get the records of your background investigation, we have a set of rules and guidelines that govern those, that govern the sharing of those. So it is used for the investigative decision, but there are very specific guidelines about how that information is used. We have specific guidelines about records retention consistent with NARA and their policies.

And a core element in the cybersecurity design of our systems, particularly as we're thinking about as we go forward, is how do we make sure we've got the appropriate protections in place for all of that information, not just Social Security numbers?

But there are very explicit policies around records retention, around records sharing, both externally within the government. Right. This information was gathered for a specific purpose. That's what it was used for, and there are guidelines around that in place.

Mr. MULVANEY. Just a quick question, and I honestly don't know the answer. But when the data was hacked that Mr. Lynch mentioned before, was it just Social Security numbers that were lost or was it other information as well?

Ms. COBERT. The information that was lost was data in people's backgrounds investigation, so it included a range of information, not exclusively Social Security numbers.

Mr. MULVANEY. Thank you.

Thank you, Mr. Chairman.

Mr. MEADOWS. I thank the gentleman.

The chair recognizes the gentleman from California, Mr. Lieu, for 5 minutes.

Mr. LIEU. Thank you, Mr. Chair.

My questions are for Mr. Evanina. First of all, thank you for your service, and I support incorporating social media into Federal background investigations.

I have a broader concern which is whether race or ethnicity play a role in security clearance denial or granting. And let me give you some context for this. Recently, four American citizens were arrested and indicted for espionage, and then all charges were dropped. These were in different cases, and it turned out that the government just got it wrong. And the one fact that was the same among all these cases is the defendants looked like me. They happened to be Asian Americans. The cases of Sherry Chen, Xiaoxing Xi, Guoqing Cao, and Shuyu Li. Their lives were turned upside down because of what our government did. The New York Times has asked our government to apologize.

I wrote a letter signed by over 40 Members of Congress asking the Department of Justice to investigate. Since I wrote that letter, our office has been contacted by Federal employees who happen to be Asian American alleging that their security clearance was denied because of their race or ethnicity. And so my question to you is, does race or ethnicity play a role in Federal background investigations?

Mr. EVANINA. Sir, absolutely not, and it's unequivocally not. I don't think there has ever been a situation where an investigator has used race or ethnicity for any determination of a clearance for a U.S. citizen, number one.

Number two, the situation you referenced, I could say that with 19 years in the FBI, I could assure you that the FBI does not conduct investigations relevant to whether your race or ethnicity comes to play.

Mr. LIEU. Thank you. Let me ask you a question about how this policy would be implemented in terms of social media. Let's say a Japanese American Federal employee has a Facebook page, and friends of this Federal employee living in Japan or relatives post on that Facebook page. Does this Federal employee become more suspicious because of that?

Mr. EVANINA. Absolutely not. And the only issue would be if on that public facing Facebook page there is derogatory or negative information that's relevant to an adjudication of investigation, will result in a followup lead. But otherwise, it would not.

Mr. LIEU. Thank you. The U.S. Government, under the Obama administration, runs something called the insider threat program, where Federal employees are asked to report on other Federal employees who may be suspicious. Is race or ethnicity allowed to be taken into account under that program?

Mr. EVANINA. Sir, first of all, the National Insider Threat Task Force is housed within my shop, National Counterintelligence Security Center. And, again, unequivocally, race or ethnicity has no part in the insider threat process or the criticality that we have across the government.

Mr. LIEU. Are Federal employees, when they're given training on the insider threat program and how to report, are they given that training about race and ethnicity playing no part?

Mr. EVANINA. Well, I think the race—any fundamental training regarding race and ethnicity crosses all boundaries, not just investigative. That's part of the Federal workforce and our fabric as Americans, number one.

But in terms of the Insider Threat Task Force, race, ethnicity, or any other type of genre of covered classes is never a part of the Insider Threat Task Force. We are—our number one mission is to identify potential insiders, spies, espionage matters, or those who seek to do harm to others.

Mr. LIEU. Could you provide my office with guidance in how you train Federal employees?

Mr. EVANINA. Absolutely, sir.

Mr. LIEU. Great. Thank you.

I've gone to a number of national security events and briefings, and I think it's not a secret that our national security establishment looks very nondiverse. And there's been articles about the

State Department having trouble recruiting people who are minorities. And I'm wondering if that has anything to do with security clearances and the inability of some folks, who are minorities, who might not be able to get them. Could you provide my office with some data or statistics on who gets security clearances based on race and ethnicity?

Mr. EVANINA. I'm sure we can, sir.

Mr. LIEU. Great. Thank you.

And with that, I yield back.

Mr. MEADOWS. I thank the gentleman.

The chair recognizes himself for a series of questions, and I'll be very brief.

Let me follow up on a couple of clarifying things. You have obviously put out this new policy, and we applaud that. We thank you for that.

Is there any particular legal reason or practical reason why we would not be asking them for their online identities?

Mr. EVANINA. Well, sir, I think as part of the SF–86 application, and when you write your name, Bill Evanina, it's asked, do I have any other names or aliases that I go by. So that's the first——

Mr. MEADOWS. Yeah, but I'm talking about online identity. So, I mean, you know, Twitter, Facebook, you know. Because I'm not going to give it in a public forum, but I have actually Twitter accounts that don't actually have my name associated with them, and yet I would tweet out things based on that. So is there any reason why we wouldn't ask for those types of things, practical or legal?

Mr. EVANINA. I don't believe it's a legal issue. I think it's a policy issue, and I think we have to have some clear differentiation between what is investigatively relevant. And we can get to those areas of——

Mr. MEADOWS. But if we're talking about social media, that would be relevant. I mean, there's no expectation of privacy, other than—well, you know, you could perhaps make the case if I'm wanting to be private about it, I'm not putting my name. But if you just ask for those online identities, would the online identities be synonymous with an alias?

Mr. EVANINA. They could be, sir. There absolutely could be, but we——

Mr. MEADOWS. So I guess if there's no legal or practical reason why we wouldn't do it, why would it not be part of your new policy?

Mr. EVANINA. Again, I will say that the policy is a start where we're going right now to get where we are.

Mr. MEADOWS. So are you willing to look at that particular component about asking for other online identities and maybe report back and your philosophy here within the next 60 days to this committee?

Mr. EVANINA. Sir, I think we're willing to look at all suspects of social media and how it pertains to the background investigation process.

Mr. MEADOWS. But, specifically, with regards to that question, are you willing to look at it and just report back? I'm not asking——

Mr. EVANINA. Yes, sir.

Mr. MEADOWS. —you to give me a definitive answer; just that you get back to this committee on what your opinion is——

Mr. EVANINA. Yes, sir.

Mr. MEADOWS. —on why you should or should not do that.

Mr. EVANINA. Yes, sir.

Mr. MEADOWS. All right. Thank you.

Ms. Cobert, I'm going to finish with you, and it's really something from in the past. And I just would like to ask you, with regards to the CIO and IG relationship, how would you characterize that from where it has been and where it is today? And if you can speak to that.

Ms. COBERT. Thank you, Congressman. Let me turn it on. Thank you, Congressman. We have been working across the agency to strengthen our effectiveness of our dialogue with the CIO, and I believe we've made real progress in a number of different areas.

We've set up a cadence of regular communications at my level with the inspector general, currently acting inspector general. On a biweekly basis we meet and get an overview of the issues. We have specific working teams that meet on a periodic basis as well, both around the CIO, around procurement. We set up that same kind of mechanism around the standup of the NBIB, given the oversight issues there and making—wanting to make sure we get those right.

So I think we've made considerable progress in terms of the dialogue, the clarity of the communications. We welcome their input on what we could be doing as better, as we welcome input from our colleagues here and elsewhere.

Mr. MEADOWS. So you would characterize it as much improved under your leadership?

Ms. COBERT. I would characterize it as much improved, yes, sir.

Mr. MEADOWS. All right. Thank you.

The chair recognizes Mr. Lynch for a closing question or statement.

Mr. LYNCH. Thank you, Mr. Chairman.

And, again, I want to thank you for being here. I want to ask you a question sort of off the grid here. I appreciate that you're making progress, and that's a good thing, and we're working together with DOD to secure our systems.

There's another issue. You know, these hackers have become so proficient. You know, this morning we got news that the SWIFT, you know, commercial bank system—I think it's 11,000 banks and companies that handle international banking transactions, they were hacked again. They were just hacked through Bangladesh and the New York Fed, which is troubling, to the tune of about $81 million. Now we find out there's another hack going on similar to that one. So they are being breached.

The FDIC, Chinese hackers, news, again, this morning, that the FDIC has been hacked. And these are entities that have fairly robust, you know, protections. And we're about to enter into this—well, we're about to debate the Trans-Pacific Partnership, and one of the provisions in that Trans-Pacific Partnership requires U.S. companies to establish databases in the foreign countries. There's about 12 countries. But, you know, one of them is Vietnam, a Communist country.

So we would have to—the U.S. companies will have to establish, physically, databases in those countries, Malaysia, Vietnam. And a lot of the banks and companies involved here are very concerned about the security aspect of this overseas.

And I just wonder, especially, Mr. Evanina, you know, I know you worry about this stuff all the time; as well, you know, Ms. Cobert, you are dealing with; Mr. Scott, you as well. What about that dimension of this? I know it's not—you know, you weren't prepared this morning to address this question, and I appreciate it if you want to take a pass, but I'm just worried about that, about it's tough enough to protect the data when it's in the United States. And now we're being asked to force our companies, if they're dealing in international trade, to actually deposit their data in these foreign countries that don't have the security protections that even we have.

Mr. Evanina?

Mr. EVANINA. Sir, I concur with your concern for cybersecurity and the need for us to be prepared to at least meet where we are in the global economy. I'm not particularly familiar with the requirements contained within this policy, so I can't speak to that. But under the purview of national security, the cyber threat is real. And I think we have to take that into consideration for anything we do moving forward, whether here domestically in the United States or any of our businesses and government operations overseas.

Mr. LYNCH. Okay. Thank you.

Ms. Cobert, Mr. Scott, you want to take a bite at that, or you all set?

Mr. SCOTT. Well, I would just say, one of the lessons learned, I think, worldwide has been that cybersecurity knows no national boundaries and, you know, concerns about cybersecurity are, you know, global. Physical location is one element, but probably in the case of cybersecurity, not the most dispositive in terms of the concerns I would have. It's more about the secure-by-design sort of notion, you know, what have you put in place and how well is it implemented, and so on. So those would be more my primary concerns.

Mr. LYNCH. Yeah, my——

Mr. SCOTT. In some cases, the physical location.

Mr. LYNCH. Right. My concern is obviously the Communist government in Vietnam is going to require access. So that was my concern. You have suffered enough.

I want to yield back. Thank you.

Mr. MEADOWS. I thank you.

And I want to thank all the witnesses for being here today. And if there's no further business before the subcommittees, the subcommittees stand adjourned.

[Whereupon, at 10:15 a.m., the subcommittees were adjourned.]

○