Senate (Select) Intelligence Committee Hearing On .., sked FINAL

March 7, 2018 5:46PM ET

TRANSCRIPT

March 07, 2018

COMMITTEE HEARING

SEN. RICHARD M. BURR

WASHINGTON, DC

SENATE (SELECT) INTELLIGENCE COMMITTEE HEARING ON SECURITY CLEARANCE REFORM

Bloomberg Government

Support: 1-877-498-3587

www.bgov.com

SENATE (SELECT) INTELLIGENCE COMMITTEE HEARING ON SECURITY CLEARANCE REFORM

MARCH 7, 2018

SPEAKERS:

SEN. RICHARD M. BURR, R-N.C., CHAIRMAN

SEN. JIM RISCH, R-IDAHO

SEN. MARCO RUBIO, R-FLA.

SEN. SUSAN COLLINS, R-MAINE

SEN. ROY BLUNT, R-MO.

SEN. TOM COTTON, R-ARK.

SEN. JAMES LANKFORD, R-OKLA.

SEN. JOHN CORNYN, R-TEXAS

SEN. MITCH MCCONNELL, R-KY., EX OFFICIO

SEN. JOHN MCCAIN, R-ARIZ., EX OFFICIO

SEN. MARK WARNER, D-VA., VICE CHAIRMAN

SEN. RON WYDEN, D-ORE.

SEN. MARTIN HEINRICH, D-N.M.

SEN. JOE MANCHIN III, D-W.VA.

SEN. KAMALA HARRIS, D-CALIF.

SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. ANGUS KING, I-MAINE

SEN. CHARLES E. SCHUMER, D-N.Y., EX OFFICIO

SEN. JACK REED, D-R.I., EX OFFICIO

WITNESSES:

KEVIN PHILLIPS, PRESIDENT AND CEO OF MANTECH

JANE CHAPPELL, VICE PRESIDENT FOR INTELLIGENCE, INFORMATION AND SERVICES AT RAYTHEON

BRENDA FARRELL OF THE GOVERNMENT ACCOUNTABILITY OFFICE

DAVID BERTEAU, PRESIDENT OF THE PROFESSIONAL SERVICES COUNCIL

CHARLIE PHALEN, DIRECTOR OF THE NATIONAL BACKGROUND INVESTIGATION BUREAU

BRIAN DUNBAR, ASSISTANT DIRECTOR FOR SECURITY AT THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

GARRY REID, DIRECTOR FOR DEFENSE INTELLIGENCE AND SECURITY IN THE OFFICE OF THE UNDERSECRETARY OF DEFENSE FOR INTELLIGENCE

AND DAN PAYNE, DIRECTOR OF THE DEFENSE SECURITY SERVICE IN THE

DEFENSE DEPARTMENT, TESTIFY

BURR: Good morning. I'd like to thank our witnesses for appearing today to discuss our government's security clearance process and potential areas of reform.

Intelligence community, Department of Defense, and defense industrial base trust cleared personnel with our nation's most sensitive projects and most important secrets. Ensuring a modern, efficient and secure clearance process is paramount and necessary to maintain our national security.

The committee will first hear from industry representatives on their perspective on the process and how it affects their ability to support the U.S. government.

BURR: Our first panel includes Mr. Kevin Phillips, president and CEO of ManTech; Ms. Jane Chappell, vice president of intelligence, information and services at Raytheon; Mr. David Berteau, president of the Professional Services Council; and Ms. Brenda Farrell from the Government Accountability Office.

Welcome to all of you. We appreciate your willingness to appear. And, more importantly, thank you for the thousands of employees you represent, who work every day to support the whole of the U.S. government.

Many of our nation's most sensitive programs and operations would not be possible without your work. I look forward to hearing from you on how your respective companies view the security clearance process and how it affects your operations, your hiring, your attention and your competitiveness. I also hope you've come today prepared with ideas for reform, where necessary.

Our second panel will include representatives from the executive branch: Mr. Charlie Phalen, director of the National Background Investigation Bureau; Mr. Bryan Dunbar, assistant director of National Counterintelligence and Security Center at the ODNI; Mr. Garry Reid, director for security and intelligence at the Office of the Undersecretary of Defense for Intelligence; and Mr. Dan Payne, director of Defense Security Services at the Department of Defense.

They'll provide the government's perspective on this issue and will update us on their efforts to improve the efficiency and effectiveness of the current system.

The purpose of this hearing is to explore the process for granting secret and top secret clearances to both government and industry personnel, and to consider potential better ways forward.

The government's approach to issuing national security clearances is largely unchanged since it was established in 1947, and the net result is a growing backlog of investigations, which now reached 547,000, and inefficiencies that could result in our missing information necessary to thwart insider threats or workplace violence.

We should also consider new technologies that could increase the efficiency and effectiveness of our vetting process while also providing greater real-time situational awareness of potential threats to sensitive information.

Furthermore, the system of reciprocity whereby clearance granted by one agency is also recognized by another simply does not work. We would all agree that the clearance process should be demanding on candidates and should effectively uncover potential issues before one is granted access to sensitive information. But, clearly, the current system is not optimal and we must do better.

I'm hopeful that today's discussion will have some good ideas and strategies that we can put into action to reform the process. Again, I want to thank each of our witnesses for your testimony today, and I'll now turn to the vice chairman for any comments he might have.

WARNER: Thank you, Mr. Chairman, and welcome to our witnesses. And I want to first thank the chairman for holding this hearing, particularly in an unclassified setting.

I believe that the way our government protects our secrets is a critical area for oversight of this committee. And, as the chairman's already mentioned, in many ways, the system that is in place, which was born in 1947 -- and I remind everybody that's when classified cables were sent by type wire -- typewriter and telex -- really hasn't changed very much.

I believe that the clearance process is a duplicative, manual-intensive process. It relies on shoe-leather field investigations that would be familiar to fans of spy films. It was built for a time when there was a small industry component and government workers stayed in their agency for their entire career. The principal risk was that someone would share pages from classified reports with an identifiable foreign adversary.

Today, in many ways, we worry more about insider threats; someone who can remove an external hard drive and provide petabytes of data online to an adversary or, for that matter, to a global audience.

And industry -- and much of that industry I'm proud to have in my state -- and industry is, by a ways (ph), a much larger partner. Workers are highly mobile across careers, sectors and location. Technology such as big data and A.I. can help assess people's trustworthiness is a far more efficient and dynamic way. But we've not taken advantage of these advances.

Just last month, at an open hearing, the director of national intelligence, Director Coats, said that our security clearance process is, in his words, "broken" and needs to be reformed. In January of this year -- and I, again, appreciate the GAO witness today -- placed the security clearance process on its, quote, "high-risk list" of areas that -- the government needs broad-based transformation or reforms.

The problems with our security clearance process are clear. The investigation inventory has more than doubled in the last three years, with, as the chairman's mentioned, 700,000 people currently waiting on a background check.

Despite recent headlines, the overwhelming majority of those waiting don't have unusually complex backgrounds or finances to untangle. Nevertheless, the costs to run a background check have nearly doubled. Timelines to process clearance are far in excess of standards set in law.

These failures in our security clearance process impact individual individuals, companies, government agencies and even our own military's readiness. Again, as I mentioned, in the Commonwealth of Virginia, I hear again and again from contractors, particularly from cutting-edge technology companies and government agencies, that they cannot hire the people they need in a timely manner.

I hear from individuals who must wait for months, and sometimes even a year, to start jobs that they were hired for. And I've heard from a lot of folks who ultimately had to take other jobs, because the process took too long and they couldn't afford to wait. To complete -- to compete globally, economically and militarily, the status quo of continued delays and convoluted systems cannot continue.

No doubt, we face real threats to our security that we have to address. Insider threats like Ed Snowden and Harold Martin comprise -- they compromised vast amounts of sensitive data. And obviously the tragedy of the shootings at Washington Naval Yard and Fort Hood took innocent lives. The impact of these lapses on national security are too big to think that incremental reforms will suffice.

Again, referring back to Dan Coats's testimony, we need a revolution to our system. And I believe that we can -- I believe we can assess the trustworthiness of our cleared workforce in a dramatically faster and more effective manner than we do today.

We have two great panels here that will help us both from the government's perspective and from our national security partners in the private sector. I'd like again to thank you all for appearing.

I hope that our next meeting -- and I hope some are listening downtown -- that the office -- the OMB, which chairs the interagency efforts to address clearances, which declined to appear before us today, will actually participate in this process.

I want to be a partner in rethinking our entirety -- entire security clearance architecture. I want to work with you to devise a model that reflects a dynamic workforce and embraces the needs of both our government and industry partners.

Thank you, Mr. Chairman. I look forward to this hearing.

BURR: Thank the vice chairman.

To members, when we have finished receiving testimony, I'll recognize members based upon seniority for up to five minutes.

With that, Ms. Farrell, I understand you're going to go first, and then we'll work right down to your left, my right, all the way down the line. The floor is yours.

FARRELL: Thank you very much, Mr. Chair.

Chairman Burr, Vice Chairman Warner and members of the committee, thank you for the opportunity to be here today to discuss our recent work on the serious challenges associated with the personnel security clearance process.

We designated the government-wide security clearance process as a high-risk area in January 2018 because it represents a significant management risk.

A high-quality security clearance process is necessary to minimize the risk of unauthorized disclosures of classified information and to help ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed.

My written statement today summarizes some of the findings in our reports issued in November and December 2017 on this topic. Now, I will briefly discuss my written statement that's provided in three parts.

First, we found that the executive branch agencies have made progress reforming the clearance process, but key long-standing initiatives remain incomplete. For example, agencies still face challenges in implementing aspects of the 2012 federal investigative standards that are criteria for conducting background investigations and in fully implementing a continuous evaluation program for clearance holders.

Efforts to implement such a program go back 10 years. We found that, while the ODNI has taken an initial step to implement continuous evaluation in a phased approach, it had not determined what the future prices (ph) will consist of or occur. We recommended that the DNI develop an implementation plan.

Also, while agencies have taken steps to establish government-wide performance measures for the quality of investigations, the original milestone for completion was missed in fiscal year 2010. No revised milestone currently has been set for their completion. We recommended that the DNI establish a milestone for completion of such measures.

Second, we found that the number of agencies meeting timeliness objectives for initial secret and top secret clearances, as well as periodic reinvestigations, decreased from fiscal years 2012 through 2016. For example, while 73 percent of agencies did not meet timeliness objectives for initial clearances for most of fiscal year 2012, 98 percent of agencies did not meet these objectives in fiscal year 2016.

Lack of timely processing for clearances has contributed to a significant backlog of background investigations at the agency that is currently responsible for conducting most of the government's background investigations. That is the National Background Investigations Bureau.

The bureau's documentation shows that the backlog of pending investigations increased from about 190,000 in August 2014, to more than 710,000 as of February 2018. We found that the bureau did not have a plan for reducing the backlog.

Finally, we found that potential effects of continuous evaluation on agencies are unknown, because the future phases of the program and the effect on agency resources have not yet been determined. Agencies have identified increased resources as a risk to the program.

For example, DOD officials told us that, with workload and funding issues, they see no alternative but to replace periodic reinvestigations for certain clearance holders with continuous evaluation. DOD believes that more frequent reinvestigations for certain clearance holders could cost $1.8 billion for fiscal year 2018 through 2022.

However, the DNI's recently issued directive for continuous evaluation clarified that continuous evaluation is intended to supplement, but not replace, periodic reinvestigations.

In summary, Mr. Chairman, several agencies have key roles and responsibilities in the multi-phase clearance process, including ODNI, OMB, DOD and OPM. Also, the top leadership from these agencies comprises the Performance Accountability Council that is responsible for driving implementation of and overseeing the reform efforts government-wide.

We look forward to working with them to discuss our plans for assessing their progress and addressing this high-risk area. Now is the time for strong top leadership to focus on implementing GAO's recommended actions to complete the reform efforts, improve timeliness and reduce the backlog. Failure to do so increases the risk of damaging, unauthorized disclosures of classified information.

Mr. Chairman, that concludes my remarks.

BURR: Thank you, Ms. Farrell.

Mr. Phillips, the floor is yours.

PHILLIPS: Mr. Chairman, Vice Chairman and members of the committee, my name's Kevin Phillips. I'm the president and CEO of ManTech International.

ManTech has 7,800 employees who support national security and homeland security. I appreciate the opportunity to participate in this industry panel and ask that my written statement be entered as part of the hearing record.

Senator Warner, including our initial outreach through NVTC, 15 companies and six industry associations have worked collectively over the last six to nine months to increase the visibility and importance of this matter and to propose solutions to help improve the process. Put simply, the backlog of 700,000 security clearance cases is our industry's number one priority.

Given the increasing challenges that we face in providing qualified, cleared talent to meet the mission demands, we consider it a national security issue and an all-of-government issue, because it impacts every agency we support.

Some quick facts: Since 2014, the time it takes to obtain a clearance has more than doubled. In our industry, the average time it takes to get a TS/SCI clearance, a top secret clearance, is over a year. The time it takes to get a secret clearance is eight months.

Top professionals are in high demand across the nation. They do not have to wait for over a year to get a job. And, increasingly, they are unwilling to deal with the uncertainty associated with this process.

As a result of this issue, the key support for weapons development, cyber security, analytics, maintenance and sustainment, space resilience -- space resilience support, as well as the use of transformational technologies across all of government, is being unserved.

Since the end of 2014, we estimate that approximately 10,000 positions required from the contractor community in support of the intelligence community have gone unfilled due to these delays.

We offer the following recommendations to help improve the backlog: First, enable reciprocity. Allow for crossover clearances to be done routinely and automatically.

Today, 23 different agencies provide different processes and standards in order to determine who is trustworthy and suitable to be employed within their agency. One universally accepted and enforced standard across all of government is needed.

PHILLIPS: Second: Increase funding. The current backlog shows no signs of improvement. We need funding to increase processing capacity to reduce the backlog we have today, while our government partners, who are working diligently to develop and implement a new system, work to develop the system of tomorrow.

Third: Prioritize existing cases. The amount of backlog of 700,000 cases has not gone down. The timelines have not improved. And we may be at a point where we have to prioritize, within that backlog, the cases that have the greatest mission impact, or that may have the highest -- or pose the highest risk to national security, based on the (ph) access to data.

Fourth: Adopt continuous evaluation. Adopt new systems that can be used across all of government, and establish a framework for which government and industry can better share information about individuals holding positions of public trust that is derogatory, so that we can better protect the nation against threats from insiders.

Fifth: From a legislative standpoint, we consider this a whole-of-government issue. Accordingly, we believe that a concerted focus from Congress is required and the oversight is needed. We support the reinstatement of the IRTPA timelines with incremental milestones. IRTPA is the Intelligence Reform and Terrorist Protection (sic) Act.

Finally, we offer that mobility and portability for clearances among the contractor community is needed. We in industry fully understand the importance of a strong security clearance process. That said, slow security does not constitute good security. Time matters to mission.

Industry is committed to take the actions needed to hire trustworthy individuals and to help protect the nation from outside threats. We appreciate the committee's leadership and the focus on this important matter.

Thank you.

BURR: Thank you, Mr. Phillips.

Ms. Chappell.

CHAPPELL: Chairman Burr, Vice Chairman Warner, members of the committee, I'm honored to represent Raytheon today before the Select Committee on Intelligence. Raytheon and our employees understand and take very seriously our obligation to protect the nation's secrets.

We submit to the same clearance process that governs our government and military partners, and we take the same oath to protect the information established and entrusted to us. Every day, our number one priority is honoring that oath while meeting the needs of our customers.

As vice president of Raytheon's global intelligence solutions business unit, I navigate the disruptions that backlogs in the security clearance process cause on a daily basis, not just for Raytheon, but for our suppliers and our industry peers, but, ultimately, for the warfighters, intelligence officers and Homeland Security officials who rely on our products and services to protect the United States.

The magnitude of the backlog and the associated delays is well documented and the metrics speak for themselves. But what metrics fail to capture are the real-world impact of the backlog: new careers put on hold, top talent lost to non-defense industries, and programs that provide critical warfighter capabilities suffer delay and cost increases.

The delays also come with a real-world price tag. Those new hires run up overhead costs while they wait for their clearance, resulting in significant program cost increases and inefficient use of taxpayer dollars. Reducing the current backlog will require immediate and aggressive interim steps, some of which are already being addressed.

Raytheon supports the government's efforts to -- to add resources and ease requirements for periodic reinvestigations. We also appreciate efforts to streamline the application process, automate and digitize information collection, provide for secure data storage and improve the related processes.

Beyond these actions, we -- we recommend eliminating the "first in, first out" approach to the investigation workflow, focusing immediate resources on high-priority clearance and low-risk investigations.

It's also critical that Congress and the executive branch implement fundamental reforms that streamline the clearance process and increase our nation's security by leveraging advances in technology. This effort should be guided by what our -- by what our industry calls "the four ones."

The first one is one application, which is a digital permanent record forming the basis of all clearance investigations, updated continuously and stored securely.

This second is one investigation, which would implement continuous evaluation and the appropriate use of robust user activity monitoring tools to facilitate a dynamic, ongoing assessment of individual risk, while securing sensitive information on protected systems.

The third one is one adjudication, which calls for streamlining and standardizing the adjudication system so the agency's clearance decision is respected by one -- by other departments and agencies. This would increase efficiency and promote reciprocity based on a consistent set of standards for access, suitability and fitness.

The fourth and final one is one clearance that is recognized across the entire government and is transferable -- transferable between departments, agencies and contracts.

We believe the implementation of these reforms will help eliminate the inefficiencies that hamstring the current clearance system, while promoting more effective recruitment, retention and utilization of government employees and contractors. And, most critically, these reforms will help close the security gaps that threaten our nation's secrets and personnel.

The modern threat environment can no longer be addressed using outdated and infrequent security snapshots that -- even the most well-intended reporting requirements, working groups and legislative deadlines have not and will not overcome the fear of change or the comfort of the status quo.

Strong, sustained leadership from both Congress and the White House will be crucial to the success of these efforts. Thank you for the opportunity to be here today, and I look forward to answering your questions.

BURR: Thank you, Ms. Chappell.

Mr. Berteau.

BERTEAU: Thank you, Mr. Chairman, Vice Chairman Warner, members of the committee. We really appreciate you having this hearing today. I would ask that my written statement be incorporated in the record in its entirety, and I'll just make a few key points here.

You heard the description of the problems and the -- and the process -- solutions, the -- the four ones: the one application, one investigation, one adjudication and one clearance.

It highlights, I think, the fact that this is really a whole-of-government problem. And -- and just look at the panel that you have following us. You don't have a whole-of-government representation on there, as you -- as Vice Chairman Warner pointed out.

The Office of Management and Budget plays a key role, both in the -- in the Performance Accountability Council and in the fundamental process across the board. In the end, though, this is a set of processes that exercises judgment and makes a decision of where to place trust.

And in that decision is a calculus of how much risk are we willing to accept. If it's zero, then we'll never issue a clearance, right? And so there's a whole level of dynamic that has to go on there, and the four ones helps get you there.

BERTEAU: What, though, can this committee and the Congress do? First is keep that whole-of-government requirement in mind. Second is, within that, there's a funding process.

So all of those 23 agencies that have separate authorities here have to provide funding to somebody who's going to do the work. Typically, today, that's the National Background Investigation Bureau.

We can't find, from where we sit, outside, a record of where that funding stands for those 23 agencies, because it's in -- it's across all the appropriations accounts, right? OMB used to track that and report that, but that's no longer available to us. It may be available to you. It should be available to you.

And I think it's important, as we look at the F.Y. '18 funding bill that we'll see end of this week, early next week -- make sure that that funding is in there, because these systems will not operate without adequate resources.

You can't buy your way out of it, though. There's got to be substantial process improvement, as well. My fellow panelists have talked about that.

But, in the meantime, you have a requirement for part of this responsibility to be moved from the Office of Personnel Management, the National Background Investigations Bureau, over to the Defense Department. And you'll hear more about that in second panel.

While that movement's taking place -- and the plan is it will take years, right -- the system has to keep going, as well. And so there's got to be both funding for the ongoing work and funding for the new capabilities inside the Defense Department. So that makes it all the more important.

My fellow panelists have mentioned reciprocity. This is a critical, critical issue. How can it be that you're cleared and acceptable for one part of the government at a certain level, and you're not cleared and acceptable at another part? And -- and the records show 23 different agencies.

But, within those agencies, there's lots of subcategories. DHS alone has a more than a dozen separate individual reciprocity determiners who can say, "You may be good enough for those guys, but you're not good enough for me." And they don't even have to tell us why, which makes it very hard for us to figure how to get out of that.

So industry can quantify its impact. You've already heard some of that. We all know there's an impact on the government, as well. Somewhere in the government, something's not being done or not being done as well as it ought to be or not being done as fast as ought to be.

We don't have that kind of information out of the government, but you've got to believe that, in fact, somewhere, a backlog of 700,000 is going to have an impact. Because this is not just contractors. This is government civilian personnel. This is military personnel. This is new recruits. All of those have -- have effects as well.

So I think the single biggest thing is access to information about what's going on, what the results are. You know, you've got a situation now where it used to be there was information made available to the public that we could rely on to prioritize our own resources. That's no longer there.

We need you to help make that information not only visible to you in the committee -- it might come to you in a FOUO kind of a status -- but visible to the public and to those of us who have to operate within that system in order to do our job supporting the government.

So, with that, Mr. Chairman, I'll conclude my remarks and turn back to you.

BURR: Thank you, Mr. Berteau.

The chair would recognize himself and then we'll go by seniority for up to five minutes.

My question's very simple. And it's -- it's this. Let's make an assumption that funding is not an issue. Why's it take so damn long? Give me -- give me the three things that make this process be so long.

Mr. Phillips.

PHILLIPS: Well, let's start, sir, with -- we have, from history, a number of agencies who have their own processes set up, and they have to go through those processes, and they're very manual. As mentioned before, the process was established during the Eisenhower administration. It's very manual.

Investigators have to go in person and write notes, rather than use tablets. They have to go through the mail to send a request to get an education check. They physically have to visit a person, versus using social media or other access points to get things done, when today's technology allows for a much more rapid way of getting decisions done without, in our view, changing the trustworthiness of the individual. That can be done greatly and significantly.

I think the second part is that people want to walk through the process and make sure, in this environment, that people are trustworthy. And the timeline is taking longer because the assurance is needed. And it's impacting the mission. And we want to make sure time is factored into the decisions, or we will not be able to defend the digital walls from outside threats.

So I think it's the process, and I think it's the need to have a more risk-based review against (ph) the mission requirements and the need to protect our nation, combined (ph), from insider threats.

Thank you.

BURR: Ms. Chappell.

CHAPPELL: Well, I would -- I would echo my (ph) -- I would echo his comments, but I would say it a little different. We are a nation blessed with very high technology. We are just not using that technology in this process.

We talked about, you know, people having to physically go and meet people. I think that it -- while that gives us some level of assurance, I think the continuous evaluation gives us a whole other level of insurance. And we should use that technology to give us more confidence in the results, as well as decrease the timelines.

BURR: I mean, basically, what you've told me is I've put more effort into understanding who my interns are than, potentially, the process does for security clearances, because you go to areas that you learn the most about them, which -- social media is right at the top of the list.

I can't envision anybody coming into the office that you haven't thoroughly checked out everything that they've said online, which is, to them, a protected space, and we all know that it's a public space. And I think what you've done is you've confirmed our biggest fear, that we're so obsessed with process and -- and very little consumption (ph) of outcome.

And I think that's how you get a backlog and -- and you can -- you can let that continue to be the norm and -- and nobody's outraged. What's the single change that you'd make to the security clearance process, if you only were limited to one? Ms. Farrell?

FARRELL: I think prompt action -- this needs to be, as some of the colleagues here have said, a high priority. And we keep hearing the words, "top leadership." There was top leadership involvement when the DOD program was on the high-risk list, from 2005 and 2011.

We saw that top leadership driving efforts from OMB, DOD, the DNI. That's what we're going to be looking for as we measure their progress going forward to take actions to come off of the high-risk list: top leadership actions and engaging with Congress to show that the -- reducing the backlog is a top priority, as well as take -- taking action to communicate that to the other members of the personnel security clearance community, as well as the -- my colleagues on the panel here. But leadership is desperately needed in this area.

BURR: Mr. Phillips.

PHILLIPS: Sir, immediately, it's funding. But, putting that aside, I think, long-term, it's one uniform standard and reciprocity. It's -- it's a big deal.

BURR: Ms. Chappell.

CHAPPELL: I would say continuous evaluation and monitoring -- you know, doing that on a continuous basis, which reduces the periodic investigations, which allows those people to spend more time reducing the current backlog.

BURR: Mr. Berteau.

BERTEAU: Do I get to use the three that they've already used, and add a fourth one to it?

(LAUGHTER)

BURR: Absolutely.

BERTEAU: Because I think -- I do think reciprocity is the top priority in that process, but I think -- using technology, not just in continuous evaluation, but in the investigations process itself.

I've had a clearance for nearly 40 years, and the guy still shows up with a pencil and a piece of paper and makes sure that the questions I've entered into the -- into the form, which are, in many cases, the same answers I've given for almost 40 years, are still what I believe, and he writes it down with a pencil, and then he takes it off and puts it into a computer system that's not compatible with anybody else's computer system.

Let's get the process down to where we're using 21st-century technology.

BURR: My thanks to all of you for your -- your candid responses. And I -- and I say that with the full knowledge of knowing that this issue is a multi-committee-jurisdictional issue on the hill.

So we've got just as much to fix up here. I -- I think some of the things that you have expressed are the results of -- of no coordination legislatively, and I think we're going to take that at heart (ph) as we move forward.

Vice Chairman.

WARNER: Thank you, Mr. Chairman. And, again, thank the panel for their, I think, accurate description.

I think it's really important that we all think about -- and I appreciate the GAO putting this on the national security high risk, because not only are we wasting taxpayer dollars by hiring individuals that then cannot do the work they're hired to do -- or, as some of the industry panels indicated, will then not take a job because of the clearance process.

And I think we particularly lose, on the government side, where people would come in and serve at a much, perhaps, lower salary than they would on the industry side, but because of the security clearance -- and I really appreciate, Mr. Berteau, your comments about the -- the use of technology.

If you can give -- let's start with you. And, at least our (ph) -- through our industry colleagues, other specific examples on -- on how, on a technology basis, we can improve this process that, again, candidly, hasn't been significantly updated since the 1950s.

Mr. Berteau, did you want to start? And then we'll go down -- specific technology examples.

BERTEAU: I think that the -- the entities that are involved in both the front end, the scheduling process, the investigation process and the adjudication process have all identified a number of places where they can bring that technology to bear.

The -- the greatest advantage I think we can take is to have integrated data across the government, so that, in fact, we've got access to everything, everywhere.

The intelligence community has made more progress here than much of the rest of the government has had. But they also have the advantage of scale. The scale is smaller and they've -- and they've the got funding and resources and the motivation to -- to do that.

I think we could give you a -- a list of specifics that you could consider as you go forward, as well.

WARNER: Ms. Chappell.

CHAPPELL: I would say, going back to my previous answer, that continuous evaluation -- a lot of this data that we -- that we go personally ask these people, you know, that are the same questions we've asked for 40 years -- that data -- a lot of that data is available in open source, but -- you know, that's available to anybody. It's a matter of public record.

WARNER: Rather than having somebody send a letter to an educational institution or...

CHAPPELL: Correct.

WARNER: ... so many (ph) personal visits. And don't you -- could you drill down for a minute on continuous evaluation, at least for secret clearance level?

CHAPPELL: Yes. So...

WARNER: It seems like it would make so much sense.

CHAPPELL: ... so, if -- if -- you know, if you go down through and look for bankruptcy -- if someone files for bankruptcy, that's a matter of public record, for example. We -- we can get that, you know, through, you know, just trolling the web...

WARNER: Without an agent going to -- or house (ph).

CHAPPELL: ... without an agent having to physically travel and then go take that information down with pencil and paper, for example.

WARNER: Thank you.

PHILLIPS: Sir, I'll give you two examples and one desired solution.

So we have one of -- one of my fellow CEOs has a contract where he has people in the green zone doing DOD work, and they cannot support, in that same, limited space, work for another department, because they have to follow an entire process to get a clearance in order to do that, and it's totally separated.

So, right across the street, they can't go in and support with a confined environment -- for two agencies to do the same thing in a -- in a very difficult environment.

Separately, we have a separate CEO. He's got a contract that does work, but (ph) the information flows to both DOD and somewhere in DHS. That individual has to fill two applications and go through two investigations to do the same job.

Industry quite often utilizes public systems that we share that are cloud-based, multilayer security. And we pay for it for ourselves. We control the data ourselves. But it is a universe (ph) -- uniform set of systems that are -- or is it (ph) available. We can make that decision.

I think establishing a uniform system that every agency who has funding can fund into and do its own processing would be very -- very beneficial, because then, those accesses would be available at the same security level for people to know what's happening, and that crossover and that reciprocity could happen just like that.

WARNER: And I think that (ph) -- just before I get a last question in for Ms. Farrell -- we need both reciprocity and portability. It -- one of the things that -- I think, one of the reasons why ODNI Coats is so -- this is so high on his priority -- he lived this experience, having sat on this committee for a number of years, being -- access to all types of information.

The amount of -- when he left the Senate and, for -- a few weeks later, when he was then appointed head of ODNI -- because there was that short-term gap, he had to go through a whole new security clearance process. That was pretty absurd.

Ms. Farrell, one of the things that I'd like you to comment on is -- what I've heard constantly is the debate from the government's side. Everybody knows this is a problem. But this, like much of G&A (ph), in terms of operations, gets pushed to the back of the line.

How do we make sure that we, as Congress, can, with appropriate oversight, make sure that agencies don't take their security clearance budget and push it to the back of the line?

Everybody acknowledges this is a -- issue and a problem. But these are dollars that don't ever seem to be prioritized, because they are not sole to mission (ph).

FARRELL: I think this is something that goes back to the top leadership, from the deputy director for management at OMB, who is the chair of the council that's driving the reform efforts and overseeing the reform efforts, and to send the message that this is a top priority, whether it's reducing the backlog or fully implementing C.E. And resources will be provided, and the agencies will follow suit.

And, if I may comment on the technology, the continuous evaluation is an area that you've heard has great promise, that could help streamline the process, perhaps be more efficient. And, as I noted, the efforts to implement continuous evaluation go back to 2008, with full implementation expected in 2010. And that has not happened.

We are encouraged by the DNI's recent directive expanding on what C.E. is. However, we still don't really know what continuous evaluation is going to comprise and when it's going to be implemented. And I think that's going to be a huge step, for the DNI to develop a detailed implementation plan of when the phases are going to occur and the agencies' expectations to implement that.

WARNER: Mr. Chairman, I'd simply say I think Ms. Farrell's comments are -- are pretty clear. We've just got to start at the top. And I'm disappointed, and I know you are as well, that OMB did not take our invitation to actually participate, since they chair the interagency council to try to move forward on this. And I think we need to get them back in, at some point.

Thank you, Mr. Chairman.

BURR: Senator Collins.

COLLINS: Thank you, Mr. Chairman.

All three of our private-sector witnesses today have been understandably very critical of the unacceptable flaws in the government's clearance process and the lack of a system of continuous evaluation. Inadequate funding has been mentioned.

I want to turn the question around. There have been three widely reported, serious breaches at the NSA, and all three involved contract employees. It is evident that relying solely on a moment-in-time shot -- snapshot of an applicant's security profile to determine clearances and secure our information and facilities is simply not working.

And I've been a strong supporter of moving to continuous evaluation, particularly following the Navy Yard shooting. But my question for each of the three of you is, what responsibility do contractors have to identify and report changes in employee behavior that may indicate a vulnerability and should trigger a review of the security clearance?

And, in at least one of the widely reported incidents involving NSA, the employees who worked with the individual were very aware of the issues that should have triggered a review of his clearance.

So I understand the role that government has and that we need to do much better. But what is your role, particularly in light of those three serious breaches, all involving contract employees?

Mr. Berteau, we'll start with you, and then move across.

BERTEAU: Thank you, Senator. That -- those are critical questions, obviously. I'd make three points there. Number one -- I know you know this, but the process is the same whether you're a government -- uniformed personnel or a government civilian or a contractor, in terms of the investigation and adjudication, processing of (ph) material.

COLLINS: I do know that.

BERTEAU: And I think that the issues that we've been talking about today, some of the process fixes, actually incorporate in them a number of the lessons learned from those very examples that you cite here, and -- continuous evaluation being the key piece of it here.

So I think that a number of the proposals, some of which are already being implemented -- although, since we don't get visible insight into that, we don't know how far that implementation is; that's a question for your second panel -- are designed to address those very same problems.

But I think there's a third piece, and the examples that you cite -- this is -- you're right. There are individuals inside who do this. But, from the company's point of view, these are people working inside a government facility.

And we frequently don't get the information about the -- or our member companies don't get the information about the employee that the government itself has. So there's got to be greater collaboration and cooperation between the government oversight mechanisms and the contractor oversight mechanisms.

This is where personnel issues, privacy issues, security issues and contract issues come together. And we've got to design it that way up front, in the contract itself. And I think we're very capable of doing that. We know how to do it; we just don't do it every time.

COLLINS: Ms. Chappell, what is Raytheon's responsibility?

CHAPPELL: So we have a responsibility to train our employees. So, yearly, we go through an employee training series that's mandated across all of our employees. And, in some cases, where we have employees sit at government facilities, they take yet a second round of training that is required by that -- by the government customer, as well, so that's two.

The second thing we do is what we call user activity monitoring. So, when you log onto a Raytheon system, you are -- it's very clear to you, it says right there on the screen that your activity is being monitored while you're on those systems.

And so we -- we have a process where we use analytic type of capabilities to look at what people are doing on the systems, to monitor their behavior, to look at -- for things that are outside their normal patterns or their normal work scope.

That data is then provided to our security operations center. And then, if it triggers an alert, we go through an investigation process. If someone comes through and, you know -- you know, says there's something going on with an employee, we trigger an investigation.

COLLINS: Mr. Phillips, very quickly, if ManTech has a group of employees working for the government in -- on highly sensitive information and many of the employees of that group -- thinks that one of the employees has gone off the rails, developed a drug problem, has financial problems, what specifically happens?

PHILLIPS: Specifically, ManTech has an insider threat program that identifies high-risk employees. And, once those individuals -- whether they hold a position of trust or -- see a behavior that we need to track, it rolls into a process that's controlled through our senior security executive, coordinated with our human resources and legal department, and overseen by myself, with board updates every quarter to make sure that we are tracking those individuals that have been identified from an insider threat perspective.

We report that information to the government. We also start monitoring their overall behavior, where appropriate, to make sure that that individual's behavior doesn't provide additional risk of harm to our employees or federal employees, or potentially increase the position (ph) of trust or breach of data to the government.

And, additionally, we spot-check people coming out of our own SCIFs for data. We want to make sure that, as a partner, we're doing everything we can. The only thing we suggest: We have to share information better about individuals who hold positions of public trust.

COLLINS: Thank you.

BURR: Senator Feinstein.

FEINSTEIN: Thanks very much, Mr. Chairman.

I'd like to follow up on Senator Collins' questions to you, Mr. Phillips. Specifically, what changes have been made by your company in the wake of Snowden and Martin?

PHILLIPS: Ma'am, since then, we've increased our insider threat process. We do more training.

FEINSTEIN: From what, to what? If you could be specific here...

PHILLIPS: Sure.

FEINSTEIN: ... that would be helpful.

PHILLIPS: I think all of government is moving towards mandating industry be a partner in this process. We already had a process in place, but what we're doing is we're making sure that every behavior -- we physically go to our program managers and we tell them, "If you or your employees see a behavior, we need to see it. We need to know."

FEINSTEIN: Well, where did you miss with Snowden?

PHILLIPS: We did not -- we would -- we did not have that event within our framework. The Snowden component, or something like that specifically, is the employee is on a federal facility, and a company cannot access the government's data to see the behaviors. They have to be visually seen by the people around that individual. We need to better share information.

FEINSTEIN: Isn't that an important point right there?

PHILLIPS: Yes, ma'am. It's very important.

FEINSTEIN: I just want you to -- because, I mean, these were big events. And they -- it's very hard for us to know the background and how it happened. So could you go into that in a little bit more detail?

PHILLIPS: Anything that has a -- is on a secured government network or secure government facility is controlled by the government, regardless of whether it's the military, federal employee or contractor. And the information flow around that is fairly limited for security reasons, but also personnel reasons.

The information-sharing program that we think is best long-term, aligning those who have positions of public trust and have agreed to that with the appropriate protections of privacy -- if they are on a network having classified information, how do we better collectively track the behaviors and actions of the individual so that we as a contract community can take the appropriate actions on that staff.

FEINSTEIN: Well, as you know, both these employees were contract employees with NSA. Have -- how closely have you reviewed the procedures? And have you made any recommendations to NSA?

PHILLIPS: Ma'am, the agency has gone through significant review. And we, as a contract community, are adjusting to meet the required additional standards to be responsive to the risks that they may have seen within their review.

BERTEAU: Senator...

FEINSTEIN: Well, maybe...

BERTEAU: ... could I -- could I...

FEINSTEIN: ... somebody could add to that, because that's a very general statement and it doesn't leave me, really, with any answer.

BERTEAU: ... if I could sort of add a little bit to that -- not necessarily the Snowden case or the Martin case, but we see, time and again, the situation where the government will tell a contractor, "This person is no longer suitable. Take them off the contract."

But they won't tell us why. They won't tell us what behavior has occurred, what has motivated them to do that. And so we're left trying to figure out what happened here, right, without the...

(CROSSTALK)

FEINSTEIN: How often does that happen?

BERTEAU: I don't have a count to follow off of (ph), because there's no database to do it. But I hear about it more than once a year. And I probably don't hear about a lot of times that it does happen.

And so you have individuals -- and it may be that the company releases that individual -- but the individual can go somewhere else. So that information sharing that should occur here between the government and the contractors involved, cutting across the security domain and the personnel and human resources domain, has got to be improved.

FEINSTEIN: Because, of the 4,080,000 national security clearances, the contractors hold almost a million -- 921,065 of those. That's a big constituency out there.

And, because it involves the defense companies, of which Raytheon is a California company that I'm very proud of that's one of them, it seems to me that the private sector has an increased responsibility, too. Ms. Chappell, how do you view that? How does Raytheon specifically view an increased responsibility?

CHAPPELL: So I think -- you know, we -- we are -- we have stepped up our training requirements around this area -- you know, more sensitivity to, you know, what has happened and making people aware.

When it's on our own networks, we have control on what we monitor and, you know, what -- where we see risk and how we escalate that and where we investigate. I think Mr. Berteau is very correct in that there needs to be better partnership.

When our employees sit on government facilities and use government networks, there needs to be more information sharing on what we can do jointly, because we don't have the ability to monitor those networks. So I think any insight we can get there is most helpful to us in -- in making sure we, you know, adjudicate through our workforce.

FEINSTEIN: Right. On -- on pages 7 and 8 -- I'm looking for your written remarks and can't find them at the moment, but you -- you make some good recommendations. Could you go into them for us, please?

CHAPPELL: On the -- on the written...

FEINSTEIN: On the -- in the written -- and let me find it. I...

CHAPPELL: Just one second, please.

FEINSTEIN: Yes. I'm sorry. Mr. Chairman, I'm sorry. My hand slipped and I lost the -- (inaudible).

CHAPPELL: So I think that was around the one application.

FEINSTEIN: That's right. The fundamental reforms.

CHAPPELL: Yeah.

FEINSTEIN: And you began with the clearance backlog of 300,000 and the one application, and it runs through. Now, this is more than a decade, as you point out, since they were first proposed.

But, to -- to make immediate progress, you say Raytheon encourages the government to prioritize and set incremental milestones for implementing government-wide reciprocity, continuous evaluation and information technology reforms. Can you be more specific about that?

CHAPPELL: Yeah. So, on the one application -- that is, the one standardized and -- you know, one standardized, one digitized, so it's available, can be shared across organizations, you don't have to fill that out more than once; one investigation to make sure that -- you know, whether it's a DOD investigation, an Air Force, Army or CIA investigation -- that that's the same investigation; they have the same standards, the same views on risk. Those can be shared across the different agencies.

One adjudication of that, so, instead of having different adjudications, you have one set of -- of adjudication process; one set of risks that that adjudication is based on, so that -- then that clearance can be -- can be agreed to and can be recognized across the different agencies; and then, clearly, there's the one clearance, you know, to make sure that that reciprocity moves across organizations.

So I think they're pretty -- they're pretty fundamental, pretty standard, pretty simple processes: one application, one clearance process, one adjudication recognized by all.

FEINSTEIN: Do you think that would...

CHAPPELL: Three strike (ph)...

FEINSTEIN: ... make a difference with the 4 million and the 600,000...

(CROSSTALK)

CHAPPELL: I think it would make -- I think it would make a huge difference because not only would it streamline the original investigation; you're not reinvestigating the same people over and over. And -- and the -- the resources required to do the reinvestigations would be focused on the backlog.

FEINSTEIN: Thank you.

Thank you, Mr. Chairman.

BURR: Mr. Berteau...

BERTEAU: Mr. Chairman, if you would indulge me for just one -- one added point, Senator Feinstein's line of questioning's really critical here.

One thing I think is important to put on the record: The member companies for PSC, and companies like Raytheon and ManTech, are very limited in their ability to get information out of the government of the status of the investigation and adjudication that's going on with the people that they've submitted into the process.

If Kevin Phillips or Jane Chappell calls the government agency that's going that, what they will likely be told is, "We can't tell you anything. Go talk to your contracting officer representative," who then has a process they have to go through internally -- not the speediest of processes -- and they may or may not get you an answer back.

We see cases where a decision has been made and not communicated to the company, in some cases, for more than six months. So there's a lot that has to be done here in terms of improving the communication back and forth. I think the oversight role of this committee, in encouraging that and getting visible results of that from the agencies involved, will be very helpful.

FEINSTEIN: Thank you very much. Would you be willing to write something up as to what both of you or three of you think would -- would be the specifics and send it to the chairman?

BERTEAU: Absolutely.

CHAPPELL: Yes, ma'am.

FEINSTEIN: Thank you. Thank you very much.

BURR: Thanks, Senator.

Senator Blunt.

BLUNT: Thank you, Chairman.

Ms. Farrell, in your testimony, you talked about the 12 recommendations I think you made to the director of national intelligence. How many of those did they accept?

FARRELL: For the majority of those we directed to the DNI, they did not comment whether they agreed or disagreed. So we -- we don't know if they're going to take action on those recommendations or not.

BLUNT: I think -- I must have read your testimony wrong. I got the impression that they had concurred with some, but not all.

FARRELL: They did concur with some of...

BLUNT: What does that mean, they concurred with some, but didn't accept them? I'm...

FARRELL: Well, they concurred with some...

BLUNT: ... going to have to (ph) get my thesaurus out here to figure out what that means.

(LAUGHTER)

FARRELL: ... they concurred, for example, with taking steps to develop a continuation -- continuous evaluation policy and an implementation. But, on other actions, they disagreed. They thought that they had already had things in play, and that no more action was necessary.

BLUNT: Which of the 12 things you recommended do you think would have the most impact on achieving the goal we want to achieve here?

FARRELL: For today, I think it would be the implementation plan for continuous evaluation. But I also have to note that there's been a lot of discussion about reciprocity. And reciprocity is statutorily required by the Intelligence Reform and Terrorism Prevention Act of 2004.

So, by that act, agencies are supposed to honor investigations that are conducted by an authorized provider, as well as adjudications from an authorized adjudicator. There's always certain exceptions, but there -- reciprocity is in statute. It just hasn't had guidance so it can be implemented.

BLUNT: And continuous evaluation, Ms. Chappell -- how does that relate to what -- you're saying a lot of the same thing: continuous evaluation using open-source data or data that's already been collected, rather than going through that process again. You want to talk about that just a little bit more?

CHAPPELL: So what we're saying is, instead of waiting from day one, when you're given your clearance, to year five, and having no investigation between that period, and then doing your periodic investigation with -- sending people out traveling around the country, doing your investigation, all through that time period, to continuously monitor data to see if there is any adverse data concerning that person and do you need to start -- you know, is that person of higher risk and do you need to pay more attention to that person sooner, rather than wait the normal five to six years for that background investigation.

BLUNT: And, if that -- if that person, like Senator Warner mentioned about the -- Senator Coats, in that brief space -- when someone has been -- has moved onto another job and is coming back, do they have to go through the whole clearance process again? They have to resubmit, again, everywhere they ever lived and...

CHAPPELL: Yes, sir.

BLUNT: Don't we have all that somewhere, if they've been cleared once?

CHAPPELL: Yes, sir.

BERTEAU: Mr. -- Senator Blunt, I've lived in the same house for the last 29 years. I've had the same neighbors on each side of me for the last 29 years. Both are former government employees with suitability determinations and clearances, as well.

Every time I fill that form out, it's the exact same information as it was the time before and the time before that and the time before that. It's already in their databases. They just make me do it again.

BLUNT: Does anybody have a reason that would justify why you'd have to do this again, if the government's already collected all this?

BERTEAU: There's an old saying, Eric Sevareid brought it out of World War II with him, called "The chief cause of problems is solutions." And, in almost every case, these elements of the process that are built in here was a fix to a previous problem.

What we've never done is the kind of end-to-end analysis of what, actually, result are we trying to get out of this and how do we design a process that gets that result.

I think what you'll hear from the second panel is, some of the efforts both that the National Background Investigations Bureau has underway and that DOD is developing a plan for will take advantage of some of that opportunity. It's just going to take a long time, and we'd like to see it speeded up.

BLUNT: And, Mr. Berteau, on one other question, are small county -- or small companies, rather, treated differently when it comes to getting their employees cleared?

BERTEAU: Unfortunately, they go through the same process. And I think they have an added disadvantage, right? If a company has substantial amount of work in the government, they may actually be able to make a job offer to a new employee and say, "We've got something we can have you do while we're waiting the year or two years it takes to get this clearance through the process."

It's very much harder for a smaller business who doesn't have the business base or the overhead capacity to be able to do that. So you make a contingency offer.

Well, if this is a critical skill -- let's say it's a cybersecurity expert who's just come out of college -- you're asking them, "Put your career on hold for an indefinite period of time. Don't get paid, right -- go do something else while you're figuring out what to do here. And then maybe we'll get a clearance at some point in time and be able to hire you."

This has two negative advantages (ph). One, it's going to reduce the number of people who are going to want to do that. Secondly, they're going to have lost their technical edge, because the system is moving on -- the cybersecurity world is moving on while they're not working in it. And so it has a double impact.

When I mention the importance of balancing risk here, there's a risk that we often don't take into account. It's not just the risk of awarding a clearance to somebody who ends up doing something wrong.

There's a risk to government missions and functions in every step of the way by not doing it in a timely way and not by having the best and brightest people on board to do that. That's got to be part of the calculus. Nobody documents that.

BLUNT: Thank you.

Thank you, chairman.

BURR: Senator Wyden.

WYDEN: Thank you, Mr. Chairman. And this has been a good -- good panel. And I'm just going to ask one question of this panel, and it's for you, Ms. Farrell.

It seems to me one of the central issues here is there is a culture where over-secrecy is actually valued and there is no accountability for excessive secrecy. So we end up with 4 million people with security clearances.

WYDEN: And I've heard my colleagues talk about the backlog question. I know that that is very important to our companies. But I think, to really get at the guts of this issue, we've got to deal with this over-secrecy kind of question.

I'd like to ask you, what, in your view, is the government doing that is most helpful in terms of reducing that 4 million number, which I think reflects that there are too many secrets out there and too many people are sitting on them?

What's the government doing about that?

(UNKNOWN): Senator, I'll start.

WYDEN: I -- I'd like to start with the GAO on it.

(UNKNOWN): OK.

WYDEN: OK?

FARRELL: Thank you. That's OK.

There's -- we have, in the past, recommended that DOD and its components -- the services, as well as the agencies -- evaluate their (ph) positions that require clearances to make sure that the clearance is required in the first place, and then have procedures in place where they periodically reevaluate those positions to see if those clearances are still necessary.

That would be a way to make sure that the requirement is correct. And most people think that clearances follow people. Clearances don't follow people. They follow the position.

WYDEN: Ma'am, I -- I want to be respectful. I know of your recommendations. I'm curious as to whether you think the government is moving effectively and expeditiously on actually doing something about it, because this strikes me -- this excessive number of security clearances -- and your recommendations are always to have these efforts to reduce them.

This has been the longest-running battle since the Trojan War. I have been on this committee -- I think, with Senator Feinstein, we're the longest serving, you know, members. And I have heard this again and again.

So what is the government doing that is actually effective, in your view, about this? Not your recommendations, which I think are very good, but what's the government doing that is actually effective, now, in terms of reducing this number?

FARRELL: Well, I think the answer is, obviously, not enough, because, if they were doing enough in terms of leadership and prompt action, they wouldn't have the backlog that they have or the -- the number of people that you're calling into question.

WYDEN: OK. I'm going to submit some questions to you in -- in -- in writing, as well. And thank you, Mr. -- Mr. Chairman. I look forward to the second round.

BURR: Senator Cornyn.

CORNYN: Thank you, Mr. Chairman.

With the hack of OPM a couple of years ago, reportedly by a hostile foreign power, countless Americans have had their privacy violated and their personally identifiable information obtained by that foreign power.

Can -- do any of you have any observations or comments about what impact that sort of lack of security for that sensitive information -- what impact that's had on the best and the brightest people who we would like to serve in these important positions?

CHAPPELL: So I'll start with that, because my personal information was some of that information that was leaked -- not only my information, but the people who I had down as references, my family members, also -- their information was also compromised.

So I think it's incredibly important that this data is -- is secured and that it goes through the same cyber process that the -- the programs that we support do.

CORNYN: Mr. Berteau, the -- you were saying how you have to fill out the same information on repetitive applications for security clearances. Well, I guess we know that foreign nations have that information, but the U.S. government apparently doesn't keep it in a place where they can use it without asking -- having to ask you each time.

BERTEAU: Senator, I -- it is my understanding that, actually, a number of steps have been taken inside the Office of Personnel Management to provide greater security. It's a question, I think, for the -- for the second panel on -- on the status of those steps.

But -- but we also have to recognize that we'll never be 100 percent secure on -- on being able to do that. And I think we have to be able to mitigate against that, as well.

I would also note that -- that it's not just the central databases that come into play here. It's all the individual things inside each of the agencies, as well. We probably are in a situation where we're going to have to be able to recognize and mitigate that as rapidly as possible.

I'm probably a little less concerned about that particular -- although, you know, I got a letter and my wife got a letter and my kids all got a letter, as well -- I had responsibility inside DOD to actually oversee the mailing of those 22 million letters.

We mailed out a million a week, and it took the better part of half a year to notify everybody. I note that that mailing occurred about a year and a half after the breach, so we also need to be able to let people know in a more timely way that their data has been compromised.

CORNYN: I just -- I don't know anything about that episode that we can be proud of -- just seems to me to be embarrassing. And, obviously, people are at risk as a result. Let me move on to ask the -- about interim clearances, the role of interim clearances.

What I don't understand is, how -- how can somebody get a -- have a sufficient background investigation to get an interim clearance? And what limitations are put on that clearance that would not be available, or that would -- would not apply to a complete clearance, so to speak?

And how -- how does that actually work, in practice, the role of interim clearances and the background investigations that are conducted to approve those?

PHILLIPS: Senator, thanks for the question. ManTech is entering its 50th year of supporting national security this year, and we have forever had interim clearances being an integral part of moving people into supporting the federal government.

As you know, the interim clearance process is a decision that's a government decision. It is not something that we as contractors can decide. We had to inform the government and let them let them make those adjudications.

We have not seen, as a company, issues with the process and how we do it. That said, one of the issues is, because of the time it takes to get a security clearance, that interim security clearance timeline is now longer than it was three years ago. So part of our suggestion is we need to move that timeline back so the time people have interim security clearances is narrowed.

The process itself is the background investigation that is commercial is done on the individual from a company standpoint. The forms are reviewed in total about the employee to make sure that -- the potential applicant -- to make sure that all information is available so that that government employer or official can make a decision whether there's (ph) sufficient grounds to grant an interim clearance, based on those facts, before the more manual investigation takes place.

In our history as a company, less than one person per year has been identified in that sequence as not being supportable to doing (ph) security work in the future.

CORNYN: Thank you.

BURR: Senator Heinrich.

HEINRICH: Thank you, Mr. Chair.

I'm going to follow up a little bit on those good questions from my colleague from Texas.

For -- for those of you in -- in industry -- and we'll start with you, Mr. Phillips -- how often have you seen a -- a TS/SCI interim clearance? Is that a common thing?

PHILLIPS: For our industry, it is not uncommon. But, as an example, out of our -- let's say 150 people doing an interim status...

HEINRICH: Yeah.

PHILLIPS: ... a vast majority of them are secret for the type of work we perform. So I can't compare it to any other application requirement.

HEINRICH: Got it (ph).

PHILLIPS: Those who are in an interim secret status have already received a secret clearance.

HEINRICH: Right.

PHILLIPS: So it's -- it's fairly narrow bandwidth (ph).

HEINRICH: Ms. Chappell.

CHAPPELL: From my personal knowledge, I don't know of interim clearances on a TS/SCI kind of clearance. Those are usually finalized.

HEINRICH: Right.

CHAPPELL: From an interim clearance, they're more on the secret side. And, quite frankly, with the backlog of clearances that we have right now, I think the risk of not doing that and -- and, you know, not being able to perform the mission is very high, so.

HEINRICH: OK. That's very helpful.

BERTEAU: Senator, in -- in my experience -- I don't -- I don't know if there -- if there's data collected on this, but -- but, in my experience, it was more common in the past. It's a lot less common today, and it has been a lot less common over the last few years.

So I think it's one of those examples of...

HEINRICH: It's probably for...

BERTEAU: ... lessons learned.

HEINRICH: ... for good reason, right...

BERTEAU: For good reason, I agree.

HEINRICH: ... for the risk that's inherent in that.

Does the government track how many interim security clearances are issued by type, by agency, by personnel type? And is there a process in place to make sure that, when that temporary access period is expired, that there's a review to say, "Whoa," you know, "Red flag, this has come to an end, we should look at this person again"?

FARRELL: I take it you want me to answer that.

HEINRICH: Yeah, if you -- if you could.

FARRELL: That information might be at the agency level, in their case management systems, but it was not at the levels that we looked at in our reviews when we worked with ODNI to collect data on the investigation time, as well as adjudication and intake for specific agencies.

HEINRICH: So, obviously, the whole of government, all the agencies aren't here right now, but that's something we should probably pay a lot of attention to.

FARRELL: Yes.

HEINRICH: For any of you want -- who want to offer your advice on this, it -- it -- it seems to me from some of the previous testimony that it sounds like continuous evaluation is really important, but it shouldn't necessary -- necessarily supplant a periodic review. It should supplement a -- a periodic review.

Is that your view across the board? And -- and, any of you want -- who want to offer your advice on that, I'd be curious to...

PHILLIPS: Yes, sir, I'll start.

So technology allows for continuous evaluation for -- 10 years ago, you really couldn't do it.

HEINRICH: Sure.

PHILLIPS: So start with that. It's a very good thing to utilize, and, over time, it will become a more and more important thing, because it can be depended on.

And, in fact, it will identify things not five years from now, but along the way, between now and five years. You know (ph), we consider it a use of technology to the benefit of national security.

Within that framework, depending on the level of trust on the C.E. process itself, the periodic reinvestigation percentages can come down.

HEINRICH: I see.

PHILLIPS: I don't see it going away, but it can be like the IRS, we're going to audit you every once in a while, versus everybody, 100 percent.

HEINRICH: So the interim period between those periodic reviews might get longer, based on a lower risk.

PHILLIPS: Yeah. And -- and there can be sample periodic reinvestigations to help inform and make sure the process is working.

HEINRICH: OK.

Ms. Chappell.

CHAPPELL: I would just say it slightly different, and I would say it focuses where the higher risk is and where you should focus periodic investigations on.

HEINRICH: Ms. Farrell, I want to ask you one more question before I run out of time here. You testified that the National Background Investigation Bureau is trying to decrease the backlog, but it has huge challenges in actually achieving this.

One of the -- the stories I've seen that I'm intrigued by that seems to be working is NBIB is taking and deploying teams of investigative personnel to specific sites for a two-month period where they'll set up shop in a dedicated workspace and they try to crank through some of those time-sensitive clearance investigations without the back-and-forth that we heard about in some of the testimony -- the travel, the inefficiencies.

This is happening right now at a couple of labs in -- DOE labs in New Mexico. It -- it seems like a rare good-news story of -- of increasing efficiency. Do you agree with that? And the -- is this a model that we should be potentially applying more broadly?

FARRELL: What we found during the review was that the bureau did not have the capacity to carry out their investigative responsibilities and reduce the backlog.

The bureau looked at four scenarios of different workforces to try to tackle this backlog. They looked at just if things stay the same. They looked at very aggressive hiring of contractors. They decided that it was not feasible for the plan where they would put so much emphasis on the contractors. In the two plans that they did look at, the backlog still would not be reduced for several years.

There hasn't been a selection, though, of which plan they're going to go with in order to reduce the backlog. So that -- that is going to be key. You can't reduce the -- the backlog if you don't have the workforce.

The other thing...

HEINRICH: I -- I don't disagree with you. I don't think your answered my question, but, well (ph), my time is over, so we're going to have to move along here, Mr. Chair.

BURR: Senator -- Senator King.

KING: Mr. Berteau, first, I want to congratulate you, because you made the key point of this whole hearing, for me. It's the opportunity cost that we should be talking about. It's the good people lost.

And that's the -- that's what brings me here today, because I know too many stories of people who just gave up, who spoke Arabic, who had visited and lived in the Middle East and, because of that, couldn't get their clearance. It was a kind of catch-22, and those are the very people that we want.

So I think that's what we have to keep focusing on. It's those immeasurable people lost, the opportunity cost that has -- has made this such an important inquiry.

Ms. Farrell, who's in charge? If John McCain were here, he'd be saying, "who can we fire?" Why is this -- why -- this is a pure management problem, it seems to me.

FARRELL: This is a management problem, and I've referred to the Performance Accountability Council, because those are the principals that are in charge of implementing the reform efforts and overseeing...

(CROSSTALK)

KING: Who are -- who's on that council? Who are the people?

FARRELL: It's the deputy director for management at OMB. It's the director for national intelligence, who is also the security executive agent, which means that person sets the policy across...

(CROSSTALK)

KING: Well, my problem with that is, any time you have a council -- and the term "all-of-government" has been used. I'm -- I'm sick of that term. That means "none of government." That's what people say when nobody's in charge.

Is there one person who has the responsibility for fixing this problem? And who are they?

FARRELL: I would point to the chair of the Performance Accountability Council, because that person does have the authority to provide direction regarding the process and carry out those -- those functions.

KING: Is that person going to be here today? Do you know?

FARRELL: I -- I believe they -- that person declined.

KING: Well, that's kind of ridiculous, isn't it? So the one person in the government that's in charge of this issue that's a very important issue isn't here, because they -- did they have to wash their hair? What -- what's the deal?

FARRELL: I can't speak for OMB, sir.

KING: Well, that's -- that's really -- that's really disappointing. OK.

Again for -- for you, Ms. Farrell: The private sector has -- has moved on from the 1940s style of doing these things. The financial sector had -- do -- does it much more quickly. Have we tried to learn from them? Has there been any effort to study how the financial sector does this, for example?

FARRELL: I do believe that the executive branch agencies have reached out to the private sector. After the Navy Yard shootings, they're -- they did a 100 -- a 120-day review.

They identified challenges within the process. There was a lot of coordination with government and non-government. Many of the recommendations that they had were recommendations that they have been working on, though, since the reform began, back with the passage of the IRTPA.

KING: Well, I would hope that we could -- we could try to learn something from the private sector, because they appear to be doing this much more efficiently.

Mr. Berteau, a technical question: The people who come to interview you, to do -- redo these security clearances -- do they carry a clipboard?

BERTEAU: I think they do, sir, and I think it's legal-size, so that it has more room on...

KING: To me, the clipboard is the sign of not being in the 21st century.

BERTEAU: I'm sorry to hear that. I actually own a couple of clipboards, and I occasionally use them.

(LAUGHTER)

KING: I used to say it was the universal symbol of authority, but, if you go into a hospital and they hand you a clipboard, they are -- they are seeking data from you that they already have somewhere else in their system.

BERTEAU: That -- that's certainly been my experience...

KING: That's the point I'm trying to make.

BERTEAU: ... yes, sir. And I think that -- that's certainly within my experience.

If I could add something on the "who's in charge" thing, I think you've -- you've hit a very key point here. There are divided responsibilities.

And some of those divided responsibilities actually spill over into the question that Senator Wyden raised about really focusing on -- we've been focusing entirely on the supply side of this equation, how do we actually move people through the process and put them into clearance.

There is a demand side of this equation, as well. And, actually, operating under the authorities granted by this committee, a previous DNI did a substantial reduction in the number of billets that required a clearance. I don't remember the exact number -- I think it was something around 700,000 that -- they eliminated the requirement for a clearance.

If you could do one thing to reduce the backlog, getting rid of the demand would be the one thing. But what we've seen over time -- and this is back to your question of who's in charge -- is other responsibilities, responses to other incidences -- the Navy Yard shooting, for example.

We see -- when I was back in the Defense Department, what I saw was, in fact, you had to practically get a clearance to get a pass to get on the base, even though there would be nothing you would ever touch in the way of classified material, once you got on.

That's out of an abundance of caution that -- we don't want somebody to be able to come on the base with a gun and be able to kill our people. There are other ways to do that, I would submit, than expanding and lengthening the background investigation process, and continuous evaluation and using 21st century technology is a key of that.

KING: But -- I'm...

BERTEAU: And the government has to do that, as well as contract...

(CROSSTALK)

KING: ... I'm running out of time, but I want to ask one more -- one more question.

Am I correct in taking from this panel that -- that these security clearances are not transferable, they're not portable? You get one in one agency, and you -- if you go to another agency, you have to start all over?

BERTEAU: It varies. There are -- there are parts of the government where...

KING: That's a disappointing answer.

BERTEAU: ... there are places where the portability is pretty robust and it doesn't take very long -- sometimes, maybe only a day or two. There are others -- Department of Homeland Security, for example -- where I believe the average to move from one to another is almost 100 days.

KING: And this is for somebody that already...

BERTEAU: Within the same department, under the same Cabinet (ph).

KING: ... I'm sorry, they already -- I can't believe what you just said. You mean a person within the Homeland Security Department who has a clearance, to move from -- from one job in Homeland Security to another job in Homeland Security, takes 100 days?

BERTEAU: Yes, sir. And it could even mean that a contractor, sitting at the same desk, moving to a different contract has to go through a new process.

KING: That's preposterous.

BERTEAU: Yeah, I -- I think that's a very nuanced and subtle word to use for it. Yes, sir.

(LAUGHTER)

KING: Thank you.

Thank you, Mr. Chairman.

BURR: Senator Lankford.

LANKFORD: I want to be able to pick up where you just left off, because that was actually one of my key questions -- was about the reciprocal agreements for clearances.

What's holding that back, that you have seen at this point -- of why the agencies don't trust each other enough to be able to handle clearances? Is this an issue of, "No, our people have to be able to do it; I don't trust your people"? Or not a common set of standards?

BERTEAU: It's probably a combination of a host of things. I think the three things that you could do about it -- number one is force a set of common standards that are the starting point.

And, even within DHS, for example, there are -- there's only statutory standards for one part of DHS. It happens to be the Transportation Security Administration, and that's a result of a different line of congressional inquiry.

Setting common standards and then reviewing and making sure that the deviations or the additions to those standards are minimized, and they have to be approved by the top leadership -- so there's a leadership question. That's the second piece that comes in.

LANKFORD: So what -- what is currently not aligned right now on our standards?

BERTEAU: I think it tends to be more in the civilian agency side than it does in the intel community and the Defense Department side. I think, there, the standards are a little clearer. But they're not clear to us. We as contractors often don't know what standards are going to be applied to the individuals we...

(CROSSTALK)

LANKFORD: Just going to push pause on that real quick.

Ms. Farrell, what would be the -- could we get a list from anyone to be able to say where are we deviating in standards -- civilian, defense contractors, whatever it may be?

FARRELL: The standards should be the same for -- there's federal investigative standards. They do not differ by category of the workforce. The federal adjudicative standards are also supposed to be uniformly applied.

There are no -- there's no data, there's no measures about the extent to which reciprocity works or does not work. This is something that we have recommended before, that there should be a baseline to determine whether or not reciprocity is -- was working and, if it's not working, then to be able to pinpoint the issues that are being discussed as to why it's not working.

Many years ago, it was believed that reciprocity was not working because agencies did not trust the quality of the investigations that someone else had done. But we don't know what the issue is today.

LANKFORD: So, when I meet with the chief human capital officers of the agencies, affectionately called "CHiCOs," those folks tell me that one of the key areas that slows down federal hiring, which, now, is over 106 days, on average, across the federal government, is this reciprocity issue.

This issue is not only slowing down and creating a bigger backlog and, as you've mentioned, Mr. Berteau, a demand issue -- that we've got to be able to go through this again and again and again for the same person -- and an incredible nuisance for the person that's actually going through it for the third time -- but it's also decreasing our federal hiring and the -- and the speed of actually getting good people on the job.

So what I'm trying to drill down on: Is this an issue of agencies having a standard across all of federal government, but they add one more, and because they've added one or two more, then we've got to redo the whole thing, rather than trusting somebody else who's already done it and we're going to just do this one additional check? What is it?

FARRELL: This is an issue of the DNI not issuing the policy on how reciprocity should be applied so that the...

LANKFORD: But reciprocity's already required of agencies.

FARRELL: It's required by statute.

LANKFORD: So it's required, but you're saying it's just a matter of releasing a document from (ph) the ODNI or from anyone else on how to actually apply what is current law?

FARRELL: Because there -- current law does state, "with certain exceptions." So it's up to the DNI to note what those certain exceptions are so that the agencies will be able to determine if an investigative (ph) can be accepted as well as an adjudication.

LANKFORD: Because, at this point, who is determining what the certain exceptions are?

FARRELL: The agencies.

LANKFORD: So they can determine, "I don't trust them," or "I don't know them," or whatever it may be, and...

FARRELL: Correct. There's some guidance out there, but it's not clear. So the DNI is working on a reciprocity policy, and we are waiting for that policy to be issued.

LANKFORD: OK, well, what is the key information gathering that is needed, Mr. -- you also mentioned this, as well -- about individuals getting onto a facility that may not need security clearances because they -- they're not going to touch documents, they're not going to see elements they shouldn't be able to see.

What -- what is the lower level that could be done faster to make sure those individuals can get access and start to do their job, but not have to go through the full check?

BERTEAU: So the DNI does have the statutory authority and responsibility for -- for the standards for security clearances. There's a second set of standards just for suitability or -- or fitness to -- to be in the job, and for the credentials to be able to access the facilities.

Those standards are governed by the Office of Personnel Management, not the DNI. And there frequently needs to be a little better mapping between these two.

I think the greatest thing this committee could do is to require regular reporting of a lot more information about this. My experience as a -- as a government official is, when I'm required to send you a report on how I'm doing, I'm going to pay a lot more attention to what I'm doing than if I'm not.

LANKFORD: True (ph). Thank you.

BURR: Do any members seek additional time? Senator Cornyn.

CORNYN: Can I just ask one more question, Mr. Chairman.

BURR: Absolutely.

CORNYN: Who in the United States government decides who is eligible for a security clearance?

FARRELL: That would be the -- usually, it's the agency of the employee that's applying for the clearance. The agency takes the investigative report and determines if someone is eligible or not.

CORNYN: Thank you.

BERTEAU: Mr. Cornyn, sometimes, there are easy decisions that are made at a lower level within the adjudication process, and sometimes there are harder calls that have to go higher up before a decision is made.

This has to do both with the quality and characteristics of the individual case, but also the dynamic of the job and how fast it's needed and what needs to come into play here.

So it can actually be calibrated a little bit in terms of who comes into play here. That's also a very good question, I think, to ask the government representatives on the second panel.

BURR: Vice Chairman.

WARNER: I just would -- again, thank you, Mr. Chairman for holding this hearing. And this has been something that I've been working on for some time, I think, getting more members engaged, because we are losing good people.

But I go back (ph) to Ms. Chappell's comments. One, if we can use technology, and two, the closer we can get -- at least at the secret level -- on one standard, one form, one adjudication and one clearance -- seems like it's kind of common sense.

And you marry the technology with continuous evaluation, and we could make real, real progress. And the good news is there's no -- you know, ODNI Director Coats and all (ph) -- I think a host of others realize this is a problem. And I, again, thank the chair for holding this hearing.

BURR: I -- I thank the vice chair. I thank all the members. And, more importantly, I thank those of you at the daises of (ph) witnesses today. Your testimony's invaluable to us.

I -- I walk away, to some degree, more optimistic than I came, because I think that the biggest issues that you've raised can be solved. And I think this is a question of can we put the right people in a room that understand, when you talk about reciprocity, what is that.

As I said to Senator King, we shouldn't be shocked. DHS is the commingling of about 37 different pieces that we moved from different areas of government, and we put it under a new agency. And given that there was a baptism by fire of the secretary, it's not unrealistic to believe that they still operate like the core agencies they came out of; they just happen to be under a -- a new banner.

So I -- I think these are all things that are doable, but we've got to have the right leadership in the room, talking about real solutions. And I think that it's the commitment of this committee that we will -- we will start and complete that process.

And, at the end of the day, hopefully a year from now, you will come back and tell us what great things have happened within government, and it will be because of your testimony today.

With that, the first panel is dismissed and I would call up the second panel.

(RECESS)

BURR: I (ph) officially call into session the second panel.

I'd like to welcome our witnesses for the second panel. We just heard from the industry on the challenges that they face and some potential solutions moving forward. We'll now have an opportunity to hear from the executive branch their perspectives and their ideas.

I understand the daunting task and job before each of you, vetting more than 4 million cleared personnel and identifying threats before they materialize. It's not easy. But we can do better than we're doing today.

As we continue our dialogue, I hope you'll speak freely, frankly and think creatively, because this hearing's not only about identifying the problem, but it's about uncovering the solutions.

I want to thank each of you for being here, and I -- I just want to reiterate what I said at the end of the last panel. I -- I actually am more optimistic right now than I was before -- before we started, because I think we've been able to clearly understand the big muscle moves.

And I think that putting the right people in the room might enable us to try to overcome some of the challenges and replace it with solutions that we would have full agreement are worth trying, or that we feel will achieve a different outcome.

So I'm not going to turn to the vice chairman. I'm going to turn directly to Mr. Dunbar, who, I understand, will begin. And then the floor will go to Mr. Phalen, and then Mr. Reid and Mr. Payne.

Mr. Dunbar, the floor is yours.

DUNBAR: Thank you, Chairman Burr, Vice Chairman Warner and members of the committee. Thank you for the opportunity to appear before you today to discuss security clearances, challenges and reforms.

The director of national intelligence is designated as (ph) the security executive agent. In this role, the DNI is responsible for the development, implementation and oversight of effective, efficient and uniform policies and procedures governing the conduct of investigations, adjudications and, if applicable, polygraph for eligibility for access to classified information.

The National Counterintelligence and Security Center has been designated as the lead support element to fulfill the DNI's SecEA responsibilities. We're responsible for the oversight of policies governing the conduct of investigations and adjudications for approximately 4 million national security cleared personnel.

The security clearance process includes determining if an individual is suitable to receive a security clearance, conducting a background investigation, reviewing investigative results, determining if the individual is eligible for access to classified information or to hold a sensitive position, facilitating reciprocity and periodically reviewing continued eligibility.

We work closely with the agencies responsible for actually conducting investigations and adjudications and managing other security programs associated with clearances. This ensures that our policies and practices are informed by those working to protect our personnel and sensitive information.

We have collectively enjoyed some noteworthy progress in security reform, including the development and implementation of multiple security executive agent directives, examples of which I've outlined in my written statement for the record.

However, as recently noted by DNI Coats in his annual threat assessment, today's (ph) security clearance process is in urgent need of substantive reform across the entire enterprise. We must quickly and with laser focus identify and undertake concrete and transformative action to reform the enterprise while, at the same time, continuing to ensure a trusted workforce.

Underpinning this reform effort must be a robust background investigation process which enables federal employees and contractor workforce partners to deliver on agency mission while also protecting our nation's secrets.

When the background investigation process fails or is delayed, mission delivery suffers, the national security is put at risk, and our ability to attract and retain the workforce of the 21st century is inhibited. Despite the hard work of dedicated, patriotic professionals who are working these issues daily, we have reached a time of critical mass which demands transformative change.

Significant challenges with the background investigation program continue to adversely affect government operations. The current investigative backlog is approximately 500,000 cases, and the average time for investigating and adjudicating clearance is three times longer than the Intelligence and -- Reform and Terrorism Prevention Act standards.

For the first quarter of 2018, our metrics indicate the fastest 90 percent of top-secret background investigations government-wide took, on average, in excess of 300 days. This is four times longer than the IRTPA standards and goals.

In addition, background-investigation-related costs have risen by over 40 percent since 20 -- F.Y. '14. The SecEA; the suitability executive agent, or SuitEA; all security organizations; and all impacted industry partners agree that this is unacceptable.

I would like take the opportunity to provide the committee with more detail regarding our upcoming trusted workforce 2.0 initiative. This initiative is designed to address the transformational overhaul I referenced earlier.

It is an enterprise effort sponsored by the security executive agent and the suitability executive agent, in concert with our partner organizations, which will bring together key senior leadership, change agents, industry experts and innovative thinkers to chart a bold path forward for the security, suitability and credentialing enterprise.

The participants, including all Performance Accountability Council principal organizations, are committed to critically reviewing and analyzing, with a clean slate and forward-leaning approach, how to accomplish the transformational overhaul which is required.

As mentioned in my statement for the record, our trusted workforce 2.0 initiative kicks off next Monday and Tuesday, 12 and 13 March, at the Intelligence Community Campus Bethesda. We look forward to conceptualizing, implementing and ultimately accomplishing the revolutionary change required across the clearance enterprise. In addition, we look forward to updating the committee on our progress.

The SecEA and SuitEA are committed to transformational overhaul in at least three areas: first, revamping the fundamental approach and policy framework. The current standards are built on decades of layered, incremental changes that have not fundamentally changed since the 1950s.

We have set the ambitious goal that, by the end of 2018, we will identify and establish a new set of policy standards that transforms the U.S. government's approach to vetting its workforce. Our objective must be to ensure a trusted workforce across government and industry who will appropriately protect vital national security information with which they are entrusted.

Second, overhauling the enterprise business process -- the current process is slow, arduous, overly reliant on manual fieldwork and does not leverage advancements in modern technology and the availability of data.

Finally, we must modernize information technology. Existing information technology constraints our ability to transform fast enough. We must leverage today's technology to connect vital national security processing required and ensure we are well-positioned to adopt tomorrow's advancing technology.

After more than a decade of incremental policy change, there is still an unacceptable operational burden on government agencies making security and suitability determinations.

We owe those dedicated professionals a high-performing process that meets the needs of our workforce and, ultimately, the American citizen. We are committed to full transparency of these efforts.

Thank you for the opportunity to appear before the committee, and I will be happy to respond to any questions.

BURR: Thank you, Mr. Dunbar.

Mr. Phalen.

PHALEN: Chairman -- excuse me. Chairman Burr, Vice President -- Vice President -- Vice Chairman Warner, members of the...

BURR: Let me thank you -- thank you in his absence.

(LAUGHTER)

PHALEN: I'll bring my clipboard later.

Members of the committee, my name is Charles S. Phalen Jr. I am the director of the National Background Investigations Bureau and the Office of Personnel Management, and I do appreciate the opportunity to appear before you today.

NBIB currently conducts 95 percent of the investigations across the federal government. The results of this mostly singular supply chain are used by over 100 agencies to make their independent adjudicative decisions.

Even those few agencies that have their own delegated or statutory authority to conduct investigations, such as agencies of the intelligence community, rely on our services in some capacity.

I'd like to start by addressing our existing investigative inventory and put some context around the numbers, which have been the subject of much media attention.

PHALEN: In 2017, we completed 2.5 million investigations of -- across all our investigative types. As of today, our inventory's approximately 710,000 investigative products. These include simple record checks, suitability and credentialing investigations and national security investigations.

It's important to note that the top-end number I just mentioned is much greater than the number of individuals waiting for their first -- their initial security clearance to begin working on -- with or on behalf of the federal government.

Of that total inventory, about 164,000 are either simple record checks that move in or out of inventory daily, or are investigations supporting credentialing or suitability determinations. The remaining inventory is for national security determinations or clearances. Approximately 337,000 of those are for initial investigations, and about 209,000 are for periodic reinvestigations.

Since we stood up 17 months ago as NBIB, we have worked to increase this -- our capacity and realize efficiencies. The stabilization of the top-end inventory over the past six months has been attained primarily because we have invested in the necessary infrastructure.

We really are approaching this challenge on three fronts: First, to recover from the 2014 loss of the USIS contract for investigative capacity, we've rebuilt both contractor and federal workforce capacity. As of today, there are over 7,200 federal and contract investigators working on behalf of NBIB. That's good. That's not enough.

Second, our investigative capacity can be significantly enhanced through smarter use of our workforce's time. Through the implementation of our business process reengineering strategy, we have clearly defined the critical process improvements that technology shortfalls needed to -- and corrections needed to support those requirements. And our decisions have been enhanced through better data analytics.

We have improved our field work logistics by centralizing and prioritizing cases, first with agencies, beginning about 18 months ago. And, more currently, we are beginning to start hubs with industry.

We have increased efficiencies of conducting and reporting on our enhanced subject interviews and implemented more efficient collection methodologies by leveraging the powers of technology to discover and gather information and to free the investigators' focus on those aspects of investigations where human interaction is still critical.

Third, we are fully supportive of the upcoming executive agent's (ph) trusted workforce initiatives. Our processes today are driven by the existing policies, some dating back seven decades, and we know from our experience that there is much to be gained through this strategic policy review effort, and we are fully behind it.

Underpinning all of this is a planned transition to a new information technology system being developed by the Department of Defense. The National Background Investigation Services, NBIS, will ultimately serve as NBIB's I.T. system to support background investigations, and will offer shared services, the end-to-end process for all government agencies and departments.

NBIB, with the support of its interagency partners, has made and will continue to make improvements to the background investigations and vetting processes. As an example, for the past year, we have offered our customer agencies a continuous evaluation product that meets today's guidance, issued by the director of national intelligence, for continuous evaluation.

As we work to reduce this inventory, we will continue to explore innovative ways to meet our agencies' -- our customer agencies' needs, leveraging their expertise as part of our decision-making process, and remain transparent and accountable to all of our customers and to Congress.

We recognize that solutions to reduce inventory and maintain the strength of the background investigation program includes people, resources and technology, as well as partnerships with our stakeholder agencies and changes to the overall clearance, investigative and adjudicative processes.

Finally, as the federal government works to implement the transition of the Department of Defense-sponsored background investigations from NBIB to DOD, we will examine our workforce needs, our capacity, our budget and work with our partners to minimize disruptions.

We have a shared interest in reducing the inventory, taking steps to effectuate smooth transition of operations. And we have a shared understanding of the importance of this entire process and its ultimate impact on national security.

Thank you for the opportunity to be here today. I look forward to the next year and I look forward to answering any questions that you may have.

BURR: Thank you, Mr. Phalen.

Mr. Reid.

REID: Thank you, Mr. Chairman, Mr. Vice Chairman, distinguished members of the committee. On behalf of Secretary of Defense Mattis, thank you very much for the opportunity to meet today to discuss a very important topic at hand.

I have submitted my statement for the record. And, sir, with your permission, I would just like to take a few minutes to amplify a couple points.

First of all, the Department of Defense fully recognizes and appreciates the necessity for security clearance reform. And we're fully committed to doing our part to develop and implement new and innovative methods for establishing and sustaining a trusted workforce in a manner which upholds the highest standards of protection for national security information, safeguarding our people and always ensuring the highest degree of readiness to defend our nation.

With the support of Congress's multiple committees and our close interagency partners represented here today, from the Office of the DNI, the Office of Personnel Management and the Offices of Management and Budget, we have, for the past some 18 months, been developing plans to transition responsibility for background investigations for our portion of the workforce from Mr. Phalen's organization, to the Defense Security Service, led by Mr. Payne.

And the chair and vice chair may recall, we met and briefed on this about 11 months ago, internally, and we've been moving out steadily. Last August, Secretary Mattis approved our plan, which was referred to as the Section 951 plan -- was tasked to us in the 2017 Authorization Act to submit a plan for this transition.

And, this past December, upon approval of the National Defense Authorization Act for 2018, this included direction to the Defense Department to implement the transition plan we submitted under the previous tasking, and to do so by October of 2020.

We are well underway to meet this objective. In fact, can project today that the initial phase of the plan -- and there's some dependencies I'll talk about, but we're preparing ourselves to begin implementing this plan later this year, in October timeframe, concurrent with the next fiscal year. And there's some conditions I'll talk about.

Our team and this interagency team represented here today -- we're all working very hard every day to put the resources and the procedures in place to make this happen. And Mr. Payne will talk about some of that in detail.

But, more than just a straight transfer of the current mission and the current method to our department, and in line with the intent of the security executive agent -- and it's (ph) just talked about, with the 2.0 initiative -- DOD is actively developing these alternative procedures for conducting background investigations, advantaging ourselves with all available technology and other things.

Our fundamental concept is to build on the existing continuation -- continuous evaluation program, which the security executive agent has already established -- to build around that and supplement that with additional tools, such as risk rating tools, which analyze individual risk, analyze risk by position and inform us of where to look and where to focus these processes.

REID: We have process for automated records checks. Some of this is in use today at NBIB to build around that, to take the shell of continuous evaluation, enhance that with other tools that give us a full, comprehensive picture and a contemporaneous basis of the risk that we are dealing with and individual risk and human risk associated with responsibilities, levels of responsibility, risk profiles and a host of other data that are connected to other programs we have, such as insider threat, such as user monitoring, such as base access, facility access -- we are in a position to aggregate that data to give us a much more comprehensive understanding of the risk than we currently have, and that is the backbone of the automated process we're referring to.

We have worked this with our colleagues here. We have shared it and briefed this to many of the industry leaders that you had in the previous panel and the organizations they represent. And there is full agreement of everyone I briefed that this methodology is viable and sufficient and goes far beyond where we are today in -- in updating our understanding of risk in the workforce to a more future-looking state.

We will soon -- I said there's a condition about when we'll start -- we will soon be submitting to the DNI our proposal requesting approval to begin phasing in the use of this process for selected segments of our workforce. And we will do this in a very graduated manner so we can assess and evaluate the results, everyone involved can understand what's taking place and appreciate where we are and accept the results.

And we will -- at the same time, we have to build up a capacity to do this on scale. So this is a ramp. The plan we submitted is a ramped plan. It's a three-part plan over three years. And, as I said, we are prepared, subject to the concurrence of the security executive agent, to formally commence this in October of this year.

This will be a long-term process, and it will be done in a graduated manner. We will build up our capacity and we will bring everyone along with us -- industry, government, congressional oversight, all of our reporting requirements, all of our accountability requirements.

We have every ability and full intent and no latitude not to uphold and not to represent what we're doing. There's nothing below the waterline that folks won't understand. We're very cognizant of this reciprocity issue and how people need to appreciate what's happening so they have trust and confidence in the system, and -- and we're prepared to do that.

We are equally mindful, as we do this, that we must continue to rely on the National Background Investigations Bureau to process the some 500,000 DOD cases that are in their inventory.

Those cases have gone into that system. We are enabling NBIB to do that now. We are the sponsor for the not (ph) -- for the I.T. system. We will continue to do that and build those tools out, all of which will transfer, but they will continue to be available to all of government and all investigative services providers in the federal government will have access to these tools and procedures that we are developing.

In the later stages of our plan, later into next year, we will begin working with NBIB to understand and implement the resource transfers. The -- the financial resources we put into NBIB are on -- on a pay-as-you-go, on a revolving fund. But the human capital, the federal and contractor workforce that supports NBIB now -- as they ramp down to a smaller population, we are 75 percent of their business load, roughly.

So, as we shift that -- we're working with them right now, and we have a commitment to provide a plan to the -- through (ph) the pack (ph) principles of what our ramp-up plan is and what their ramp-down plan is. And, obviously, those need to be in harmony.

We will continue to rely on them to work down the inventory, and we will support and enable them to do so. And -- and I would just add here they've done a tremendous job of dealing with a very difficult set of challenges with the inventory that -- that Mr. Phalen inherited when he took that job, and -- and we're very much appreciative of what they're doing.

I can't underestimate the complexity the -- of this endeavor. This is -- as I said, it's about a $1.1 billion enterprise. We have a volume of 700,000 cases a year that they process for us. There's some 8,000 to 10,000 people that do this.

And all of this is -- will be in motion as we phase and implement this plan, keeping them whole and viable with a re-scope mission and establishing our ability to do our mission, which would then be benefited by the fact that we have control of our own initiation process, the submissions piece, the investigations piece and the adjudications, and then -- very important going forward -- the follow-up, the continuous vetting, continuous evaluation foundations that I already discussed.

We're working on this every day. We have great teamwork. We appreciate the support of Congress in this endeavor. And, sir, thank you again, and I look forward to your questions.

BURR: Thank you, Mr. Reid.

Mr. Payne.

PAYNE: Mr. Chairman, Mr. Vice Chairman, members of the committee, thank you very much for this opportunity to -- to speak with you on -- on this topic. You have my written statement. I'm not going to go into that. And I'll try to keep my comments as brief as possible, because I know you have a lot of questions.

I will say that I am the individual who's going to be responsible for executing the mission in -- in DOD for background investigations and -- and begin to build that mission.

As a result of that, Charlie and I have to work -- Mr. Phalen and I have to work very closely with each other, and our teams have to work very closely with each other, so that we -- we do this in a manner that doesn't hinder NBIB's ability to -- to work down the backlog, while at the same time increasing our capacity to pick up these investigations.

That being said, and in view of the -- the previous panel that was here and the comments that came from the previous panel, I am responsible for industry security currently. While we do not do the background investigations ourselves -- it's Mr. -- Mr. Phalen's organization that -- that does that -- we initiate the background investigations.

I am the individual who grants interim security clearances and takes them away. I am also responsible for the execution of -- of DOD's continuous evaluation program, and -- which, from my perspective, has been greatly successful and is the way of the future. We have to go down this route if -- if we are going to make the necessary changes to make this process better.

In addition to that, the insider threat programs for -- for DOD -- I own the Defense Insider Threat Management Analysis Center, which is where all of the insider threat concerns in DOD come to, and -- and we work with the individual agencies within DOD to resolve those -- those particular issues.

All of those things combined, as Mr. Reid outlined a -- a few minutes ago -- all of those things combined are things that we did not have back in 2004, 2005, when DOD had the initial mission for -- for background investigations. We have them now. That is the way of the future. That is the way that we have to go.

If we are to make any -- any progress in making this -- this program faster and making this program more secure, we got to look at a -- a different methodology of doing this. It has to -- we have to utilize continuous evaluation and automated processes, many of which Mr. Reid outlined in -- in his statement.

But, in addition to that, we have to look at the standards. We have to change standards. If we are to do this successfully, we have to change the standards. And -- and that -- that's going to result in some big decisions on our part. And those big decisions pertain to how much risk we are willing to accept.

PAYNE: As Mr. Berteau in the -- the previous panel stated, we're never going to be able to reduce the risk to zero unless we stop hiring. Obviously, we can't do that, and there's always going to be risk involved in the investigative process. There's always going to be risk involved in the security clearance process. What we have to determine is how much risk we find acceptable.

And thank you very much.

BURR: Thank you, Mr. Payne, and thank you to all of our witnesses.

Again, we'll recognize members based upon seniority for up to five minutes. Recognize myself first.

I want to tell you a story. Story starts about 10 years ago. A 22-year-old graduates college -- never any plans to work for government -- gets offered a job, civilian at DOD, and couldn't be more excited. Parents were more excited than he was -- job, paycheck, things that you hope they're going to find -- and then, a process of 11 months of security clearance.

You know, it gets back to some things that were said in the first panel, and I don't think that I'm an exception. That happened to be my son. Here's a kid that is incredibly excited to work for government, work where he did, ready to go. And, after 11 months, you know, he wonders whether he made the right decisions.

He -- he didn't lose his skills, like some will do today, if it's technological. But the question is, how much of that initial passion for working for government do you lose, from the standpoint of the (ph) retention down the road?

So understand, I -- I get it firsthand why we've got to accomplish what you've set out to do. It is unacceptable to this next generation, just the fact that things go so slowly. I say that with full knowledge of -- knowing I'm still talking about the federal government and there are some things even Congress can't change.

But the reality is that we can do much better. And, Mr. Reid, I thank you for your brief almost a year ago. The fact is the timeline's about exactly where you told us it was going to be.

We're excited to see the rollout. Mr. Payne, a lot of pressure on your shoulders, I -- I get that. But we can't go forward unless we do this. I know the commitment of -- of Dan Coats, and I don't think that that's going to change, as -- as long as he's there.

And I think, now, we're matching it with a desire by members of Congress to make sure we not only identify those things that need to be changed, but we accomplish those solutions. So I think that we've -- we've got good partners.

Mr. Reid, Mr. Payne, this is to you. Are there additional authorities that you need to accomplish this rollout and eventually fully move the system to what you have designed?

REID: Senator, from an authority standpoint, the -- section 925 of the current NDAA gives us -- reinforces the secretary's authority, in the first instance, to conduct background investigations, which was a plus. It also provides direction -- not so much authority -- for us to consolidate other elements within the department, which also is very helpful.

BURR: Let me ask it a different way, if I could.

REID: Yes, sir.

BURR: Is there anything in federal statute today...

REID: No, sir.

BURR: ... that hinders your ability to change your review process the way you think it needs to be done?

REID: Not that I'm aware; not in statute. Now, we are wholly dependent on Director Coats and his leadership to approve, as I outlined, our alternative process. And -- and -- and the secretary cannot -- Secretary Mattis cannot do that unilaterally.

We are beholden to the security executive agent and the suitability executive agent for the standards they set and the process they control. And we don't have a problem with that process.

We're eagerly looking forward to participating in the trusted workforce 2.0, because it comports to the plan that we've already set out to -- to conduct. So I do not believe there's anything in federal law that is an impediment to what we want to do, sir.

BURR: Mr. Dunbar, I'd also ask you to go back and make sure, from an ODNI standpoint, that there's not some statute out there that is going to pop it's ugly head up and say "Well, you know, this does make a lot of sense, what we're doing over here, but you can't do that until we change this statute."

If we've got things to change, let us know now, so that we can -- we can implement this on the timeline that's designed.

DUNBAR: Yes, Senator. Absolutely.

BURR: Now, I -- I should have said this at the first panel, and I'll -- I'll say it now. I'm not adverse to additional investigators. I'm not adverse to increase in funding. I'm -- I am adverse in doing either of those things before we change the system.

So, you know, until you change, it's hard to truly evaluate what the need is going to be, what the cost is going to be. I am hopeful -- and I think, Mr. Reid, this is your intent -- that this takes the timeline for security approval and drives it down.

Can you give us what your goal is, from the standpoint of the timeline? If, today -- if, nine years ago, it took 11 months, I can't imagine what it is today for that similar TS/SCI (ph) individual. What's your goal now?

REID: Yes, sir. The established goals for each level of clearance are attainable under our plan. But, more -- better than that, under our plan -- currently, for a secret reinvestigation, the guideline goal is 145 days. It's taken about twice that long.

Under our plan, our vision is that that periodic reinvestigation, as it's currently conducted, does -- does not exist, that a contemporaneous continuous vetting process would be implemented in place of that.

Now, there will still be deliberate, face-to-face sort of re-upping of -- of employees. It's not autopilot. But the monitoring and the reporting, which we're already doing in our -- in our program now, will be the backbone.

So the answer to that question is the goal is to eliminate the requirement currently existing for periodic reinvestigations at all levels. We have some work to do to get -- be on the first level.

BURR: What can I tell that next 22-year-old who wants to be a civilian DOD employee and is getting ready to go through the background check -- 22 years old, out of school, never lived anywhere but school and home? How long is it going to take to process him for clearance?

REID: Again, under the current process, that ranges from 200 to 400 days. Under the future process, it's perfectly attainable to get down to -- in the current guidelines, which are, for top secret, 150 days. But we feel it can go much lower with the -- with the automation and the -- the tools that I described, sir.

BURR: OK (ph).

Vice Chair.

WARNER: Thank you, Mr. Chairman.

I think we've heard a lot of commonality, from the first panel, to the second panel, in terms of goals. And it's not a new problem, but I -- I look at just the last -- performance over the last couple of years. We've had doubling of the backlog.

WARNER: And, for Mr. Phalen, while you say it's stabilized, I don't hear -- and I'm going to come to you in a couple of minutes -- when are we going to actually get it down.

We've had a doubling of the costs. We have everybody using the term, "continuous evaluation," yet we seem to have not commonality on that or how we're going to get there. We have the notion of increased technology, but, again, I don't see a timeline presented.

We see, in certain areas -- for example, the financial sector, where there are enormous security concerns -- they have been able to implement tools like continuous evaluation using increased technology.

And I get the frustration on the DOD side to say, "We got to split this up." But we're talking about an effort to go -- if we accept some of the industry's interest in terms of one application, one investigation, one adjudication and one clearance, it seems like we're going in the opposite direction.

So I'd like to hear from Mr. Reid or Mr. Payne how we make sure, if we go through this process, we're not going to simply create more duplication, less portability, less reciprocity than what we have right now, which, again, I'm first to acknowledge, is not working.

REID: Yes, sir.

The application, the standards and the -- are federally directed. There is one. There is one standard. What we are embarking on and preparing to implement is an alternative methodology to reach those standards.

Now, in parallel, these guys talked about everyone getting together and looking at the standards. If they change, they'll change for everybody. We're not creating a new standard. We're not creating a new application.

We are automating, behind the application, the process that we go through to collect the data that's relevant to form the basis of a background investigation that becomes the basis of an adjudicative decision, a determination. We're not changing the standard, sir.

WARNER: Recognizing that you are the vast majority, how are we going to make sure the goal of reciprocity and portability takes place as you build this new system?

REID: In the very first instance, sir, that will be by adhering to the guidelines set by the executive agents in everything we implement. We do not have a unilateral authority to change that process without the executive agents' concurrence. So we will align our process to their standard.

WARNER: It -- respectfully, I mean, it -- I know you're trying to head us in the right direction, but it -- it sounds a lot of process words, rather than specific guidelines, timetables, and how we're going to get there.

Let me just -- and I -- while I share the chairman's concern about simply throwing money at it -- but my understanding is there -- an awful lot of agencies -- they kind of build this into their G&A, and they don't continue to prioritize funding, so that the funding that is even supposed to be there isn't getting there.

So I don't think we ought to throw more dollars. But I do think we need to make sure that agencies make this a priority within their funding scheme. And I hope DOD, which has gotten a very generous bump up in the last budget -- you know, if you take this on, it would be very disappointing, at least to this -- this senator, if we came back and said, "Well, we didn't have the dough to do it."

Let me go to Mr. Phalen. I mean, Mr. Phalen, I -- stabilizing at 700,000 is not acceptable. It's just not acceptable. I'd like to know when we're going to start seeing those numbers driven down on the backlog.

And also, Senator Heinrich raised issues on the earlier hearing about new techniques that some of the government labs were using in terms of hub -- for example, hubbing interviews. Why is it taking so long to try to implement what seems to make common sense in terms of hubbing interview?

I've got an area like Norfolk, Virginia, where we've got huge numbers of people trying to -- waiting for clearances. What can we -- what can you talk -- what can you say specifically about using these tools that seem to be working in DOE kind of across the breadth, in other areas where there's concentration of federal employees, like Norfolk in my area or northern Virginia in my area?

PHALEN: Taking all those...

WARNER: Start -- and start with how we're -- you know, how we're going to drive that 700,000 backlog down -- not stabilize it, drive it down.

PHALEN: Right.

So, starting one step even further behind that, when I first joined this organization, 17 months ago, the capacity to conduct the work that we were required to do was insufficient to conduct that work, period.

And that's why, as you saw in the first few months after we stood up, that inventory continued to rise, as opposed to beginning to stabilize. When we reached the point where we began -- where we have the same capacity that we had in 2014, when this all fell apart, that's a way station along the way to reach that point of stabilization. It's not the endgame.

In one sense, I'm proud we hit that stabilization point, but I'm not proud that we have not brought that inventory down. Our goal is to bring it down.

Last week, I noted to a committee on the other side, the House side, that we are looking at, potentially, as much as 15 percent to 20 percent reduction by this time -- not by this time, by the end of the -- of the calendar year.

That's still not sufficient. But it will be -- it will be -- by itself, it will begin to drive that number down. It will probably take us a couple of years to get down to a level that is much more effective.

The -- along the way, we are trying a number of things. We've talked about technology. We need to be able to get information, collect information more reliably, more quickly, through technology, as opposed to shoe leather, as was mentioned in the previous session.

The problem is getting to some of those sources right now, particularly law enforcement services, is not as easy as one would hope, and we still have to put a lot of -- lot of people on the street to find police records in relevant areas. We're continuing to work on that closely with the police agencies at the state, local, federal, tribal level to continue to do that.

You talked about hubbing. We've started that with the Department of Energy as a surge, rather than hubbing, about 17, 18 months ago. In Los Alamos, it looked very promising. We have -- since that point, we have done a number of things that are both hubbing and surging. One is more concentrated than the other.

Most recently, we finished one in Wright-Patterson Air Force Base in the Dayton area. We recognized a -- increased -- or increased efficiency of somewhere in the low 40 percent -- a positive note that -- in other words, what would normally be an hour's worth of work, they were finishing in 36 minutes, as a rough estimate. They were far more productive in that hubbing area.

You mentioned the area around Tidewater. We are actually beginning a session in Tidewater on April 1st. We've pooled (ph) together all of our -- all the federal agencies that are down there, all the DOD agencies that are down there and pooled together all of our assets, both staff and contract investigators, and we're going to focus on that area.

But that is one of probably about eight or nine that I could mention, just in the last year, where we have actually done this and found very positive results -- Certainly, Dayton; San Antonio, out in Nevada; Tinker Air Force Base, Oklahoma -- Oklahoma City; I mentioned Tidewater.

And one that I think is going to be very promising to us on two fronts -- one is we've been working with our -- with industry directly to find areas not by company, but by geography and by program -- to find those areas in the country where we can -- we can, again, focus our resources -- places like Southern California; places, again, like Tidewater; like the gulf -- sorry -- Space Coast in Florida where we can bring that together and work with industry to bring -- to focus our energies down there.

PHALEN: A second part of that is, to follow on to a comment that was made, I believe, by one of the early panelists, it's clear to me from both our current work and my last experiences in life that industry collects an awful lot of data before they put somebody in for clearance -- before they even decide to hire somebody.

And we need to find a way to leverage the work that they have already done, accept it and build it into part of the process and -- and not have to go back and ask those same questions.

And that will, by itself, reduce a lot of time in collection and effort. That's sort of a high-level view, and I hope that gets to some of those points you mentioned, sir.

WARNER: Curious -- you didn't mention the national capital region as one of these areas that would be a recipient of a hubbing area, since this is the greatest concentration of the need for clearances.

PHALEN: Interestingly enough, I asked that question yesterday and spoke to the folks in charge of the activities in this area. We are -- in the Washington, D.C. area, for work that has to be done in the Washington area, we are actually pretty close to being up to speed in the Washington, D.C. area.

It is other parts of the country that -- where the -- where somebody's background may take them to other parts of the country, where it is not as up to speed as it ought (ph) to be.

WARNER: I'll be happy to send a lot of my friends in the contractor community to you on that path. They don't believe that -- that fact.

PHALEN: Understood.

BURR: (OFF-MIKE)

LANKFORD: Thank you, Mr. Chairman.

Mr. Reid, has DOD done its own background investigations and work before, and then handed that back over to the whole of government?

REID: Yes, sir. Prior to 2005, we had responsibility for our background investigations at what's now the Defense Security Service, sir.

LANKFORD: So what's the lesson learned there? So why -- why is this time going to be better? Because, last time, it was turned over, and then, now, it's coming back. Give me the key lessons learned.

REID: So Mr. Payne touched on one of those, sir, and that is having a comprehensive process in place to deal with the volume and the scale of investigative items.

The continuous evaluation tools that we have now are different -- the (ph) risk rating and automated records checks, additional tools that we are developing to streamline the submission process within the department.

If you look at the current process and you look at past practice, there's a high percentage of drag in the system between submission and investigation just to get the submission clean and get all the data. Well (ph), we have tools in place already to improve upon that.

I talked about the streamlined background investigations and then the centrality in the -- you know, in this -- positioning of our consolidated adjudications facility, which did not exist that -- at that time, either.

So we have in place -- or we will have in place, when we move investigations back, all three pieces of this enterprise: submissions, investigations and adjudications, all under a single organization with the authority and the resources and the mission focus.

And I would just say, currently, sir, Deputy Secretary Shanahan -- the number one reform agenda for him is this clearance reform. Secretary Mattis -- firmly, firmly, actively involved in pushing us to better solutions and to make this functionality not a back-office thing that someone does in the department, not an administrative thing, but the security focus that exists in the leadership team now.

I can't say what was in 2005. It could not be any higher today, and we have the pieces aligned to put this into action.

LANKFORD: So give me the -- give me two goals that are the nickels and noses-type goals here. Will this drive down cost? And will this speed up the process?

REID: Yes and yes.

LANKFORD: Give me a ballpark of what that means.

REID: In terms of speeding the process, again, current -- current timelines, we're experiencing 150 or so days for a secret-level reinvestigation. We will eliminate that requirement completely, so there's a time improvement there.

Current background investigation field activities, field work -- our studies and our pilots and everything we've put into place now, using aggregated data tools that I've talked about, can get us 90 percent of everything we're getting now from the field investigation on the front end, and then the tools can focus on the last 10 percent.

We will still have to go out and do some field work, but 90 percent of the field work can be handled through automated processes. So that's -- will drive down the -- the capacity needed to do those field investigations and therefore drive down the cost per unit that we currently provide to OPM.

LANKFORD: Right. And you had said first-time approval is still at 150 days -- it's still your assumption, first time, new person, new hire.

REID: That's the reinvestigation. But a current -- currently, it's about the same for the initial secret -- at the secret level.

LANKFORD: And you assume it's going to still stay that 150 days?

REID: Pardon me, sir?

LANKFORD: You assume it'll still stay 150 days? The -- currently, it's 150 days. You assume, when you transition it over, it will still be 150 days for a first-time hire, brand new investigation?

REID: No, sir. No, that's the current standard.

LANKFORD: Right.

REID: I don't know today how fast we'll be able to do a secret. My anticipation is it can be done in a matter of days. There's processes in place now to gain access to certain programs and facilities, even here in the D.C. area, that run a series of automated checks that are very thorough, and it takes 20 minutes.

I don't know that we're going to be at 20 minutes. And you always are going to have things you have to go check.

LANKFORD: And, back to the chairman's question, when he talked about the 22-year-old, when he asked you a specific on that, how long it's going to take -- that's when you gave him the answer, the 150 days. So I'm trying to be able to (ph)...

(CROSSTALK)

REID: That's the -- that's the current standard, sir. I apologize.

LANKFORD: OK. All right. So you're thinking it's not going to be 150 days; it could be a couple of weeks?

REID: Absolutely. At secret level, absolutely. No reason why that can't be.

LANKFORD: OK. Mr. Payne, do you concur on that?

PAYNE: I do. I think some of the things that we have in place right now -- again, as Mr. Reid outlined, using continuous evaluation -- maybe I want to finesse that a little bit -- continuous evaluation, as opposed to continuous vetting.

So continuous evaluation, a program set up by the -- by the DNI, is designed to look at -- look at the risk in between periods of reinvestigation. When we talk about continue -- and they have seven -- seven data sources that they're requiring every agency to -- to utilize when they do continuous evaluation.

When I talk about continuous vetting, I'm looking at expanding that into other data sources, data sources within DOD, other data sources within the U.S. government, other data sources within the public sector that -- we can pool (ph) all those things together, many of which are required already for the secret-level reinvestigations, and do those on a continuous basis.

And, if we're doing those things on a continuous basis, there is no need to do a reinvestigation on someone at the secret level unless you come up with derogatory information. So that's where the significant savings is going to be.

LANKFORD: OK. Thank you.

Thank you, Mr. Chairman.

BURR: (OFF-MIKE)

KING: Thank you, Mr. Chairman.

I've been surprised in this hearing that we haven't had to talk much about money. Mr. Phalen, do you have adequate or -- and -- and Mr. Reid, is -- are there are adequate resources in terms of money and people?

Is it -- is this just management and automation? Or are there shortfalls in terms of the number of people necessary to -- to do these -- to work down this backlog?

PHALEN: So, in the current process, in our current operation, we are -- we operate in a working capital fund, a fund -- a revolving fund. And agencies that wish to have investigation done give us the money to have the investigation done.

So, from our standpoint, it is "Here's the money, do an investigation." So we're not short of funding to do these investigations on our end, right?

I think a better question would be, are the agencies that need to have an investigation conducted funded appropriately to -- to identify the money to send to us to do the investigation?

KING: And are there sufficient personnel? Are there people that -- this -- our economy's pretty tight. Are there people -- is there a shortage of qualified people to do this work?

PHALEN: There -- the high end of folks to do the investigative work in (ph) -- as a population is stressed, at this point, to -- to hit beyond where we are, although we have encouraged our suppliers and ourselves to continue hiring.

But -- so, today, there are -- nearly adequate, but we still have much more work to do. And, if we don't change today's processes -- some of the things you've heard already -- then we will still need to continue hiring beyond all that, and that puts even greater stress on the total number of people we have to do it.

KING: So that's an additional imperative to seek technological productivity increases.

PHALEN: Yes. Yes. It's to make the current people more productive and to reduce the need for having people in there. Yes.

KING: I -- I think this could go to any of you all, so (ph) I'll address it to Mr. Reid. Is the portability that we've talked about part of this sort of revamped plan, Mr. Phalen, Mr. Reid, to consider that factor so that we don't have to re-do these tests?

Let me ask a specific question. We heard about DHS, where you might have to have a whole new -- whole new investigation to go from one job to another in the same agency. Does that -- please tell me that doesn't happen in the Department of Defense.

REID: No, sir, it does not. But we have a single adjudication facility. We're all under one roof. And DHS -- aggregation of independent agencies that were brought together in DHS are still operating it differently. But we -- we have for years had a single adjudication facility within the department. And external to the department, because...

(CROSSTALK)

KING: So the -- so the clearances are portable within the Department of Defense?

REID: Absolutely, sir.

KING: And is this a -- is this -- is the portability issue in other agencies part of this reinvention that's going on?

PHALEN: Portability -- the interesting part is that the -- is a -- mostly, today, a singular investigation. Any agency can use the investigation we do to conduct an adjudication (ph). But it is up to that agency to do the adjudication.

Of the example you heard earlier, within DHS, with the same set of facts, they may decide to ask for more information, ask for re-adjudication, and then...

KING: So -- so this -- so portability isn't a part of the overall structure of the -- of the new system. It's -- it's an agency-by-agency decision whether they will accept -- whether they will do reciprocity.

PHALEN: I'd say it's less about structure and more about both empowering them and encouraging them to -- to accept the -- the decisions made by others in previous lives.

So a decision made by one agency -- for the second agency to accept that that first agency probably did a pretty good job and was honest about how they approached it and to accept the -- the results of that first investigation and not -- there may be (ph) another question, but not ask a lot more about, not reinvestigate -- not -- I'm sorry -- not reinitiate an investigation.

KING: Thank you.

Mr. Reid, why is it that it's taking so long, has taken and apparently will take so long, to transition from the OPM to Department of Defense? Why -- that -- you're -- you were talking about 2020, I think, and it started last year.

REID: Yes, sir (ph).

So the -- the Defense Authorization Act requires us to implement the plan by October 2020. We intend to implement the plan in October of '18. We -- projecting a three-year, three-phase plan, starting at the secret level.

KING: So you're going to bring it in on time and under budget?

REID: Well, it says start by 2020. So we will start now, and it doesn't say -- it didn't tell us how long to finish. But we submitted a three-year plan, so, logically, the expectation is we take three years.

When we moved it out of DOD last time, it took more than five years. And it's more complicated. But I -- to short-answer your question, we want to do it in a phased, deliberate and graduated way. We have to keep our partner agency whole. They support a lot of other agencies in the government, and they rely on us to do that.

It will help them work down their inventory. Once we start processing new cases separately, that will drive down the new work that goes to Mr. Phalen, if tens of thousand cases -- of thousands of cases a week that we are providing them now -- we will turn off that spigot, help that with -- help with the backlog as we build up our capacity and capability.

KING: I'm out of time, but, Mr. Payne, very quickly, you -- you used a phrase that struck me. You said, "We have to change the standards." What did you mean when you said that? Do you mean lower the standards?

PAYNE: I don't necessarily mean lower the standards. But we have to choose (ph) -- so the federal investigative standards dictate what steps have to be taken to achieve a secret-level security clearance or a top-secret-level security clearance. So, again, as -- as has been outlined, we -- we...

(CROSSTALK)

KING: You said (ph) it's the steps that might have to be...

PAYNE: That's correct.

KING: ... compressed, not necessarily...

PAYNE: Not the adjudicative standards, necessarily.

KING: OK.

PAYNE: The investigative standards.

KING: That's what I needed to know. Thank you very much.

Thank you, Mr. Chairman.

BURR: Senator Wyden.

WYDEN: Thank you very much, Mr. Chairman.

I have a question for you, Mr. -- Mr. Phalen. I've made a special focus of my work, during this Russian inquiry, the "follow the money" kinds of questions. I want to ask you a couple of questions relating to that.

For you, I think, Mr. Phalen, question is, should someone who fails to disclose financial entanglements with a foreign adversary be eligible for a security clearance? That is a yes or no question.

PHALEN: I'm not sure I have a yes or no answer for you, sir. I -- I believe it would -- it would play a prominent role in a decision as to whether that individual should be granted a clearance, and it is not an inconsequential question to ask.

WYDEN: But how -- how is it not an up or down, yes or no? We're talking about significant financial entanglements with a foreign adversary. Shouldn't somebody who fails to disclose it -- I mean it's one thing if it's disclosed and you have a debate and, like you say, there's (ph) balancing.

But failure to disclose seems to me a different matter altogether. So I gather you don't think, necessarily, that somebody who fails to disclose a significant financial entanglement with a foreign adversary -- shouldn't be denied a security clearance.

PHALEN: That is not what I meant to say, sir.

WYDEN: Well, go ahead, tell me what you mean to say.

PHALEN: So under -- under the adjudicative standards -- and I -- and I would defer, also, to Mr. Dunbar to reply to this, as well (ph) -- under the adjudicative standards, there is nothing that says, "If you do this, you can't have a clearance."

It -- it says to the adjudicator to take into account all that you know about this individual, make a decision regarding their candor, regarding their entanglements, regarding their families, regarding crime, regarding all sorts of things, and make a decision.

I would say that the scenario outlined would play a prominent -- be a prominent thought to be considered during the adjudication. But there's nothing to -- in today's standards says any of those things by themselves are disqualifying. It would be an -- a very important piece to consider.

WYDEN: Do you believe it ought to be disqualifying?

PHALEN: I would have a hard time overcoming that.

WYDEN: Great. Thank you. OK.

Mr. Dunbar, question for you. Jared Kushner's interim access to top secret SCI information has raised a variety of questions. Under what circumstances should individuals with an interim clearance get that type of access? That's for you, Mr. Dunbar.

DUNBAR: Senator, as we've heard earlier today with the industry panel, interim clearances have been used throughout the government for some time -- many years. They -- there are two specific governing documents for interim clearances. And the -- the guidance that's out there now allows interim clearances at the secret level, as well as top-secret level.

There are situations called out in the guidelines which speak to urgency of circumstances and those types of ideas about how -- when someone might be granted an interim security clearance.

DUNBAR: I believe an example that would be applicable here is an incoming administration, which has the need to onboard personnel and get them in positions as soon as possible, in order that they can perform the duties of (ph) their function.

In regard to Mr. Kushner's specific case, the DNI sets policy, standards and requirements. As Mr. Phalen has stated, each individual adjudication -- and this is contained in the Security Executive Agent number 4 -- is treated based on the whole-person concept in which every particular piece of information, whether positive or negative, past, present -- all of those things are factored into the adjudication.

As Mr. Phalen has stated, in my opinion, the issues which you've raised, Senator, would be issues which would need to be thoroughly vetted in the course of the investigation. I have no reason to doubt that the Federal Bureau of Investigation would not (ph) investigate each and every issue very fulsomely.

WYDEN: Let me ask one other question.

During our open hearing -- in fact, I think it was "Worldwide Threats" -- the vice chairman, to his credit, mentioned the security clearance as being central to the question of protecting sources and methods.

I asked FBI Director Wray, with respect to Rob Porter, how that decision was made. I mean, when did the FBI notify, you know, the White House? And it was clear, when you listen to Director Wray's answer, it did not resemble what John Kelly had actually been saying to the American people.

So I'm still very concerned about who makes decisions at the White House. And, with regard to White House personnel, in your view, Mr. Dunbar, who would make the decision to grant an interim clearance holder access to top secret SCI information?

DUNBAR: Senator, that decision would be made, in my understanding, by the White House office of personnel security based on an investigation conducted by the FBI.

WYDEN: My time -- my time's up. I would only say I'm not so sure, as of now, who actually makes that decision. Because we've heard Mr. Kelly speak on it. I understand the point that was made by, you know, all of you who are testifying. I think it still remains to be seen who would make that decision to grant an interim clearance.

I'm over my time. Thank you for the courtesy, Mr. Chairman.

BURR: Before I turn to Senator Harris, Mr. Phalen, since you do most of these right now, is it unusual or is it acceptable that, if an individual who's filed for security clearance finds out they left something off their application -- are they offered the opportunity to update that for consideration?

PHALEN: Yes.

BURR: So, if somebody left it off, they could add it on, and that would be considered in the whole of the evaluation?

PHALEN: Yes, it would be, and at any time during investigation. What we frequently find is two scenarios. Number one is, "I just forgot when I was filling out the SF 86 to put that on there" as an individual issue. And there are times when we -- we will go in and conduct the investigation, have the face-to-face conversation...

BURR: So that's actually happened more than the one instance that Senator Wyden referred to?

PHALEN: We find it happens with some regularity.

BURR: Thank you.

Senator Harris.

HARRIS: Thank you.

Mr. Phalen, it's important, I think, for the public to understand why these background checks are so important to determining one's suitability to have access to classified information. Can you please explain to the American people why these background checks are so important to national security?

PHALEN: Yes.

So taking a background check, in addition to both the investigative piece and then, ultimately, a decision by a government agency to grant that person access to information or have some level of public trust, the -- we owe it to -- I think we, as a government, owe it to the American people and to the American taxpayer to ensure that people who are working in the national security arena and in areas where there is a public trust -- that we have done everything we can, within reason, to determine that that person can -- that that trust can be placed into that person.

And I know, in an earlier part of the conversation, early -- earlier hearing, there was a conversation about should we reduce the number of people that have clearances.

I think there's not so much a counterargument to that, but I -- when we have people in -- across this particular environment, in the earlier panel, where they have access daily to national security information, secrets that give this country an edge in -- in war and peace and other sorts of things, and at the same time, we have our industrial partners that we work with that are building all of those tools, that help us fight those wars or keep that peace, do we -- and this is a very simple thing I've said in other venues -- do you want to have less trust in the guy who is turning bolts on an F-35 assembly line, or more trust?

My argument is we probably want more trust, rather than less.

HARRIS: And, in addition to the trust point, isn't it also the case that the Code of Federal Regulations lays out 13 criteria for determining suitability, not only to determine who we can trust, but also to expose what might be weaknesses in a person's background that make them susceptible to compromise and manipulation by foreign governments and adversaries?

PHALEN: That is correct. This is a process that is both looking at history to ask if you have already -- do you already have a record of betraying that trust, and, perhaps more importantly, both for initial investigations and for the continuous vetting or continuous evaluation portion, to say what is changing in their lives and how do we predict whether they are going to go horribly bad before they get that far.

HARRIS: So there are 13 criteria, as I've mentioned. One is financial considerations. And I'm going to assume that we have these 13 factors because we have imagined scenarios wherein each of them, and certainly any combination of them, could render someone susceptible to the kind of manipulation that we have discussed.

So can you tell us what we imagine might be the exposure and the the weakness of an applicant when we are concerned about their financial interests, and in particular those related to foreign financial considerations?

PHALEN: So, in a nutshell, it would be an individual who has entangled themselves, whether it's foreign or not, but -- in financial obligations that have put them in over their head.

And, oftentimes, this causes people to make bad decisions -- bad life decisions. And, in some of these cases, we've found, from the history of espionage, it causes them to decide, "Well, I've got something valuable here. Let me sell it to somebody."

HARRIS: And how much information is an applicant required to give related to foreign financial considerations?

PHALEN: They're required to identify foreign financial investments, foreign financial obligations, foreign property. And...

HARRIS: Foreign loans?

PHALEN: That would be a financial obligation, yes.

HARRIS: Of course.

PHALEN: Yes.

HARRIS: And, when we talk about foreign influence and it is listed as a concern, what exactly does that mean in terms of foreign influence? What are we looking at?

PHALEN: It would be, "How am I, or am I, influenced by either a relationship I have with someone who is foreign, a relationship I have with an entity that is foreign -- that could be a company; it could be a prior or coexisting citizenship I have with a foreign country; it could be a family member who is a -- is someone from a foreign country -- how much influence any of those things would have over my judgment, as to whether I'm going to protect or not protect secrets in trust."

HARRIS: And, given your extensive experience and knowledge in this area, can you tell us, what are the things that individuals are most commonly blackmailed for?

PHALEN: It is not -- I'd have to go back and do some more research. The instances of blackmail by people committing espionage is not as substantial as the incidence of people who simply made a bad decision based on financial or other entanglements. And they just make a poor decision and decide that "My personal life is worth more than my country."

HARRIS: Right.

And then I have one final question, and this is for Mr. Payne. According to press reports last fall, you said, quote, "If we don't do interim clearances, nothing gets done."

You continued to say, "I've got murderers who have access to classified information. I have rapists. I have pedophiles. I have people involved in child porn. I have all of these things at the interim clearance level, and I'm pulling their clearances on a weekly basis."

This obviously causes, and would cause anyone great concern. And -- the problem, of course, being that the inference there is that interim clearances don't disclose very serious elements of someone's background.

So can you please tell us, when we also know, according to press reports, that there are more than 100 staffers in the executive office of the president who are operating on interim clearances, what we are going to do about this?

PAYNE: I will say that the length of time that someone stays in an interim capacity has to be limited as much as possible. Just to give you an example, from DOD's standpoint -- and my -- my area of jurisdiction right now is industry, cleared industry -- last year, we issued 80,000 interim clearances to -- to industry.

Currently, there's about 58,000 people on interim clearances. If you look at the timeline that they have been involved or they have had their interim clearances, they -- it ranges anywhere from -- from six months, to two years.

But, if you look at just last year, in terms of interim clearances -- and let me give you some -- a couple of statistics here -- 486 people from industry had their clearances denied last year. Of -- their main security clearance, their full security clearance -- they were denied.

Of those, 165 of those individuals had been granted interim clearances. Now, during the process of the investigation, information was developed during the investigation that resulted in us pulling the interim clearances of 151 of those individuals, and the remainder were individuals who did things after they received their interim clearances.

So the risk -- you could see the risk that is involved with interim clearances and a need to reduce the amount of time that we have somebody in an interim capacity as much as possible.

HARRIS: I agree. Thank you.

BURR: Vice Chair.

WARNER: One, I appreciate the panel. And I appreciate your answers in the first panel, as well. This is a high, high-priority issue, I think, for all of us, and is remarkably no-partisan. We've got to get this improved.

I will leave you with one -- because we've -- it's been a long morning already, I will leave you with -- all with one question for the record, because it was raised in the first panel, but we didn't get a chance to raise it today, and I'd like to get a fulsome answer from each of you.

I would argue that, particularly in an era of more and more open-source documents, we have to take a fresh look at the need to make -- need to have over 4 million-plus people actually have to go through a clearance process of any type, and particularly the tremendous growth to -- of top secret clearances, versus simply secret.

So I'd like to hear you -- back in writing from all of you, what can we do and what would be your policy recommendations so that we could not have so many people actually have to funnel through on the demand side on a going-forward basis, where more and more information is going to be out?

Thank you, Mr. Chairman. Thank you again for holding this in an open setting.

BURR: I thank the vice chairman. I thank all of the members.

This is one of those issues that the membership of this committee has been extremely engaged on. And I want to thank those first -- the first panel members who chose to stay and listen to the government witnesses. I -- you know, I'm always shocked at the number of people that have the opportunity to testify and stay, and choose not to do that. So I really respect the ones that do take the time to do that.

I thank all four of you for not only providing us your testimony today, but for the jobs you do. Mr. Payne, you've got a big job. And, Mr. Reid, you've led this charge. Mr. Phalen, you walked in one thing (ph) -- not many people would take the job.

(LAUGHTER)

And you have -- you have performed as well as one can do. And that's faced with losing 80 percent of your business down the road -- knowing that.

Mr. Dunbar, I'm not sure you knew that you'd signed up for this when Director Coats asked you to come in, but this is -- it's important.

And, as we've chatted up here, as other members have gotten an opportunity to question you, we're really confident that this might be a model that we're beginning to see that we can replicate, and that the energy between you and Mr. Phalen, that exchange, is going to happen, and that there's a real opportunity, then, for Director Coats to coalesce the rest of government towards this model.

The one thing that -- one word that didn't come up in the second panel -- might have come up once or twice -- that came up frequently in the first one was reciprocity, because there's nothing that either one of you are doing on both ends where it solves the problem of reciprocity within an agency, or from agency to agency.

And I can tell you, we've got a security officer that got her security clearance at the State Department, but, when she came to be security officer for us, the State Department said, "We don't have accreditation with the CIA." So she had to physically go pick up her paperwork and take it to the agency to be recognized. You'd think, in 2018, something like that wouldn't exist.

And it's bad enough that it does, but I think, when we look at what -- why are we doing this, you know, it's really not to solve that problem. It's to make sure that the next generation of workers that are going to come through the pipeline actually want to do it and can do it and they do it in a timeframe that they're accustomed to.

BURR: It always mystifies me that somebody's willing to share their entire life story, because they do, right, Mr. Phalen? Everything's out there for -- to be -- be exposed, because they believe in what they're doing.

And I want to make sure the next generation has just as much passion about doing this. We wouldn't be quite as involved as a committee, if it wasn't for the passion of the vice chairman. He has been relentless on this.

And I think it's safe to say that the committee -- and I say this to you Mr. Dunbar -- I will -- I will take up with Director Coats that (ph) -- I will offer to Director Coats the committee being involved in the issue of reciprocity and how we bring agencies together to work through some of those things.

It's not that the director doesn't have the authority to do it, or -- I think he's in full agreement with us. But, sometimes, having a -- a congressional piece involved in those provides the director a -- an additional stick that he might not have without us. So I'll make that offer to Dan, that we will be involved to that degree.

Mr. Reid, I -- I hope that your history with us, which is at least annual updates, if not faster -- that you will continue those and that this committee will have a -- a real inside look into the success of the model your setting up.

Much of what we're able to accomplish, from this point forward, is because of the investment that you've made not only today, but prior to this, and we're grateful for that. With this, this hearing's adjourned.

END

Mar 07, 2018 17:46 ET .EOF