S. HRG. 118–431

OPEN HEARING: PERSONNEL VETTING, SECURITY CLEARANCE REFORM, AND TRUSTED WORKFORCE 2.0

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JULY 10, 2024

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

57–024 WASHINGTON : 2026

SELECT COMMITTEE ON INTELLIGENCE

(Established by S. Res. 400, 94th Cong. 2d Sess.)

MARK R. WARNER, Virginia, *Chairman*
MARCO RUBIO, Florida, *Vice Chairman*

RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS S. KING, JR., Maine
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, JR., Pennsylvania
KIRSTEN E. GILLIBRAND, New York
JON OSSOFF, Georgia
MARK KELLY, Arizona

JAMES E. RISCH, Idaho
SUSAN M. COLLINS, Maine
TOM COTTON, Arkansas
JOHN CORNYN, Texas
JERRY MORAN, Kansas
JAMES LANKFORD, Oklahoma
MIKE ROUNDS, South Dakota

CHARLES E. SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
ROGER F. WICKER, Mississippi, *Ex Officio*

WILLIAM WU, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

JULY 10, 2024

OPENING STATEMENTS

WITNESSES

SUPPLEMENTAL MATERIAL

OPEN HEARING: PERSONNEL VETTING, SECURITY CLEARANCE REFORM, AND TRUSTED WORKFORCE 2.0

WEDNESDAY, JULY 10, 2024

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:54 p.m., in Room SH–216 of the Hart Senate Office Building, in open session, the Honorable Mark R. Warner, Chairman of the Committee, presiding.

Present: Senators Warner (presiding), Rubio, Wyden, Bennet, Casey, Gillibrand, Kelly, Cornyn, Lankford, and Rounds.

PROCEEDINGS

OPENING STATEMENT OF HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Chairman WARNER. I want to call this open hearing on security clearance reform to order. I welcome today's Executive Branch witnesses. It's good to see all of you again. Apologies for starting a little bit late. The vote got started a little bit late.

So, we will get at it. Our witnesses today are the Honorable Milancy Harris, Acting Under Secretary of Defense for Intelligence and Security; Mr. David Cattler, Director of the Defense Counterintelligence and Security Agency, DCSA; the Honorable Dr. Radha Plumb, Chief of Digital and Artificial Intelligence at DOD; and the Honorable Stacey Dixon, Principal Deputy Director of National Intelligence PDDNI, representing ODNI as the government's security executive agency.

Today, the Committee will get a status update on efforts to improve how the government conducts security clearances for our national security workforce. As many of you know, we have long prioritized the need for fundamental reforms in this area. That's because we need Intelligence Community, community personnel and others who hold security clearances to be vetted effectively and expeditiously to ensure classified information is properly protected. We also need to balance this with the IC agencies' urgent need to quickly bring on board the very best people needed to staff sensitive positions. And that's obviously increasingly important in this challenging world.

Now, when I first got involved in this, and it may have been somebody who used to work on this Committee's staff, Jon Rosenwasser's, fault. A series of folks came to me from the consulting industry in Virginia. I didn't think that I would be a decade

in. It's been almost a decade since we started this. I knew it would take some time, but I did not realize this pursuit would be a career path. But the truth is the need for reform was clear.

Our legacy vetting system was anchored in a system that was set up literally in the 1940s and 1950s. Usually with the workforce at that point, once they got cleared, they were there for life. Very little mobility between agencies or with the private sector. And it focused on periodic, time-based reinvestigations that were almost done all by paper and in person. And that meant that people waited way too long to get clearances and, frankly, it allowed a lot of mistakes to happen.

Then in 2014, the OPM data breach highlighted the system's structural failures, and it nearly collapsed. The backlog for investigations swelled to, I think, my number here is as high as 750,000 stuck in limbo. And at that point to get a top-secret clearance took on average about two years. That's crazy. Today, with nudging from Congress and frankly bipartisan nudging from this Committee, the backlog has been significantly reduced to a steady state of about 200,000.

However, and that's the good news, over the last nine months we've seen what literally is a disaster unfold with the national background investigation systems in this, which is supposed to deliver the IT backbone for the government's Trusted Workforce 2.0. The way forward, which frankly if we don't get this right, the whole security clearance reform process crumbles.

I know we've got mostly folks who follow this stuff, but there may be some for whom this doesn't roll quite off their tongues regularly, but NBIS is supposed to enable key components such as continuous vetting. We've moved from episodic, every five years vetting, to using technology for a continuous vetting process.

So, both, better process, but it doesn't require the kind of effort of every five years with all the staffing required. And we're supposed to recognize, we've got to have more workforce mobility. We've got to realize there's got to be reciprocity between a security clearance at one agency and another.

And again, NBIS was supposed to be the linchpin of this whole transformation. When the Committee last heard a hearing on security clearance reform in March 2023, we were told—and other than Stacey, I think most of the rest of you were not involved at that point—we were told that NBIS was making great progress in meeting developmental milestones. Since then, we've learned that NBIS has been plagued with problems stemming from poor leadership, poor Executive Branch oversight, a lack of clarity about requirements, and questionable contract and program management. And to just kind of drive this home, NBIS was supposed to be delivered in 2019. We're in 2024 at this point and, unfortunately, with not a lot of clarity in sight.

This is not the only place where big software development projects have run afoul. I think all of the Senators up here have dealt with students and parents over the last year who've had to do the updated FAFSA system in terms of financial student aid. It's been a disaster in terms of the rollout. We've seen problems oftentimes with our veterans' health care systems. But at least one

of the items we're going to talk about today meets the level of inefficiency of any of these prior screw ups.

So, NBIS was supposedly—just to give you a data point—NBIS was supposedly to be completed by 2019 at an estimated cost of $700 million. Yet, five years later, we are not fully operational—$850 million has been spent on NBIS. In addition, and we just got this updated from GAO today, another $850 million on trying to deal with some of the legacy systems. And while there is a plan that we will actually get this completed over the next 18 months, which will put us into late 2025, calendar year 2025, it's still uncertain what the balance of getting this done will cost.

I know getting these new systems right is hard, but it shouldn't be this hard. The truth is this kind of screw up and this kind of inefficiency is what robs so many of our citizens of their trust in government. Now let me add, and again, I know there's a 90-day review that's been done. I'd like all of our witnesses to tell us about what happened during that review and what we're doing on a going forward basis.

Today, we're going to need some firm commitments about when we're going to see the delivery of those capabilities. And that again, Mr. Cattler, the DCSA customers have been waiting for—literally for years. We've got to get this right. We've got to make sure that the good men and women who want to join the IC are not put off by the enormous time that it takes to get a clearance.

We also have got to get the whole implementation. I think we're roughly 1.5 on our Trusted Workforce. We've got to get it to 2.0. We've got to make sure that continuous vetting, workforce mobility, clearance reciprocity, and timetables are met. I also want to add in my questions a little bit of an update on commercial SCIFs, which is something that I think, post-COVID, that we need to see.

I apologize again for the length of my opening, but it's a really important issue. And I'm grateful for you all being here.

And I turn it over to the Vice Chairman.

OPENING STATEMENT OF HON. MARCO RUBIO, A U.S. SENATOR FROM FLORIDA

Vice Chairman RUBIO. Thank you. Thank you to the witnesses for being here. Last year we held a hearing on this topic, and I stated at that time that the clearance process and the ongoing reforms are at the fundamental core of protecting our security and our Nation's most sensitive assets: our capabilities and information.

And you know, it's the job of this Committee to ensure that our intelligence is secure at least from——. That's our job from a Congressional oversight perspective. And so, it's with serious concern that we're back here a year later in what I believe is a position worse off than we were a year ago. And I'm hoping that I hear from testimony today that that's not the case.

We had the 2014 Chinese hack into the Office of Personnel Management. The next generation security clearance IT system, the National Background Investigation Services, was expected to be online by 2019. It's now 2024. We don't have full NBIS utilization, no termination of expensive and old legacy security clearance systems, and already at the tune of more than $1 billion per year.

And look, I recognize these IT systems require upgrades, but in this case, with all this expensive security clearance legacy systems still online, we have no timeline for full utilization being finalized. And an opt in or opt out confusing option for any federal department or agency. And so, I want to be persuaded why this isn't waste and redundancy and a serious lack of ownership and accountability.

So, I sort of end where we begin and that is, our oversight responsibility as a Committee is to protect our Nation and to make sure that our Nation's most sensitive secrets are being protected while at the same time enhancing our workforce. So, we've got to be able to protect our secrets and make sure the people that we're bringing in are properly vetted, but we also have to be able to bring in the best people we possibly can into the workforce. And it's essential to these efforts that the timely and secure means of recruiting, onboarding, and retaining cleared personnel exists. And so, I'm hoping that I can hear something today that makes me feel better about everything I've just said. Because when I compare where we are today to where we are a year ago, I think it's gotten worse, not better. So, thank you for coming.

Chairman WARNER. And again, for my colleagues, open hearing. The Committee's process says we do five minute rounds and by order of seniority.

With that, Secretary Harris, I think you're going to get us started. Thank you.

STATEMENT OF MILANCY HARRIS, ACTING UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY, U.S. DEPARTMENT OF DEFENSE

Secretary HARRIS. Chairman Warner, Vice Chairman Rubio, and Distinguished Members of the Committee, thank you for the opportunity to testify about the Department's progress on the initiatives underway to improve and enhance the National Background Investigation Services, or NBIS, program and implementing Trusted Workforce 2.0 reforms.

I am pleased to join the Honorable Dr. Stacey Dixon, the Principal Deputy Director of National Intelligence; David Cattler, the Director of DCSA; and the Honorable Dr. Radha Plumb, the Department's Chief Digital and Artificial Intelligence Officer. Thank you all for the partnership in getting NBIS back on track.

NBIS is critical to the Department's and the Federal Government's implementation of Trusted Workforce 2.0 initiatives. NBIS will be the end-to-end IT infrastructure that enables our security, suitability, and credentialling experts to conduct comprehensive personnel vetting, from subject initiation through background investigation, adjudication, and continuous vetting.

Although the Department has successfully deployed some key capabilities in the eight years since the program started, we are significantly behind in delivering the complete, end-to-end NBIS that has been promised to Congress and our customers. For instance, we promised and have yet to deliver background investigation capabilities to support the updated Personnel Vetting Questionnaire, a shared data layer to promote information sharing and reduce du-

plicative costs, and shared service capabilities such as adjudication case management for our federal customers.

Last year, my office became aware of a number of issues which, when explored, revealed significant impediments to delivering NBIS on the expected timeline. When I became the Acting Under Secretary in March of this year, I initiated a 90-day sprint effort focused on understanding the state of the program, the issues resulting in delays in delivering capability, and charting a path to recovery. A cross-functional team from across the Department, as well as my colleagues from DCSA and CDAO, are here today, but also our CIO and acquisition experts, began that effort on April 1st and have worked together closely to develop a way forward.

Our plan includes several actions intended to return the NBIS program to a path to success. First, we are acting to improve oversight and governance going forward by ensuring we are making decisions at the appropriate level. That includes elevating the program decision authority from DCSA to the Under Secretary for Acquisition and Sustainment. We are also elevating program sponsorship to the Under Secretary for Intelligence and Security. Lastly, we are creating a robust governance process that will allow us to translate requirements from our interagency customers while providing the necessary protections to prevent cost, schedule, and performance erosion.

DOD also has new leadership and experts in key positions responsible for NBIS development. Along with Director Cattler, DOD brought in both a new program executive officer and a new NBIS program manager. The new program manager joins us with a wealth of expertise and experience in delivering through agile methodologies—something lacking in past NBIS program management. We have also enlisted expertise from the Defense Digital Services under our Chief Digital and Artificial Intelligence Office. Dr. Plumb will testify today to DDS's focus on modular data architecture, building the right reams, and adopting digital transformation best practices, all of which will be instrumental in strengthening the NBIS program.

Combined with improved oversight, new leadership, and greater technical expertise, we are moving forward with several initiatives. The program is fully focused on Agile software development with strong involvement from our users to ensure timely feedback and value assessments of product deliveries. To support this, we are updating foundational documentation to clearly outline roles and responsibilities, establishing the program's core capability requirements in support of Trusted Workforce 2.0, and driving improvements across the board. These efforts will result in more robust, transparent, and reliable cost, schedule, and performance metrics, improving trust in future delivery of capabilities. Recovery is not quick. This will be a months-long exercise to build a foundation enabling the Department to deliver NBIS.

Despite the issues, the Department has successfully enrolled its entire national security population into Continuous Vetting, or "CV." CV is an effective model that relies on automated record checks and the reporting of relevant information from components to enable the near-real-time identification of risk. Our data indicates we are identifying potentially concerning behavior signifi-

cantly sooner than traditional periodic reinvestigations. This early detection enables a strengthened security posture, supporting our critical missions across the Department. Additionally, within the Department, Trusted Workforce 2.0 policies are driving robust information-sharing between our agency insider threat hubs and the personnel vetting enterprise, allowing us to better identify and mitigate potential risks.

In closing, the Department of Defense remains committed to the NBIS program and providing secure and effective personnel vetting processes, services, and systems so that government agencies and members of our Nation's industrial base have confidence in their trusted workforce. While we cannot undo the missteps of the past, I am confident that we are on the path to success for NBIS. It is of paramount importance that the Department regains and maintains the trust of Congress in these efforts if we are to maintain strategic advantage over our adversaries.

I thank the Members of this Committee for your strong support of the Department of Defense, and I look forward to answering your questions.

[The witness's testimony was interrupted by a failure of the audio system and was not fully recorded. The prepared statement, which she read from, follows:]

Statement for the Record as prepared for the Honorable Milancy Harris
Acting Under Secretary of Defense for Intelligence and Security
At the United States Senate Select Committee on Intelligence
July 10, 2024

(As of 1700 07/08/2024)

Chairman Warner, Vice Chairman Rubio, and distinguished members of the Committee, thank you for the opportunity to testify about the Department's progress on the initiatives underway to improve and enhance the National Background Investigation Services, or NBIS, program and implementing Trusted Workforce 2.0 reforms.

I am pleased to join the Honorable Dr. Stacey Dixon, the Principal Deputy Director of National Intelligence; David Cattler, the Director of DCSA; and the Honorable Dr. Radha Plumb, the Department's Chief Digital and Artificial Intelligence Officer. Thank you all for the partnership in getting NBIS back on track.

NBIS is critical to the Department's and the Federal government's implementation of Trusted Workforce 2.0 initiatives. NBIS will be the end-to-end IT infrastructure that enables our security, suitability, and credentialing experts to conduct comprehensive personnel vetting – from subject initiation through background investigation, adjudication, and continuous vetting.

Although the Department has successfully deployed some key capabilities in the eight years since the program started, we are significantly behind in delivering the complete, end-to-end NBIS that has been promised to Congress and our customers. For instance, we promised and have yet to deliver background investigation capabilities to support the updated Personnel Vetting Questionnaire, a shared data layer to promote information sharing and reduce

duplicative costs, and shared services capabilities such as adjudication case management for our Federal customers.

Last year, my office became aware of a number of issues which, when explored, revealed significant impediments to delivering NBIS on the expected timeline. When I became the Acting Under Secretary in March of this year, I initiated a 90-day sprint effort focused on understanding the state of the program, the issues resulting in delays in delivering capability, and charting a path to recovery. A cross functional team from across the Department – as well as my colleagues from DCSA and CDAO here today, but also our CIO and Acquisition experts – began that effort on April 1st, and have worked together closely to develop a way forward.

Our plan includes several actions intended to return the NBIS program to a path to success. First, we are acting to improve oversight and governance going forward by ensuring we are making decisions at an appropriate level. That includes elevating the program decision authority from DCSA to the Under Secretary for Acquisition and Sustainment. We are also elevating program sponsorship to the Under Secretary for Intelligence and Security. Lastly, we are creating a robust governance process that will allow us to translate requirements from our interagency customers while providing the necessary protections to prevent cost, schedule, and performance erosion.

Statement for the Record as prepared for the Honorable Milancy Harris
Acting Under Secretary of Defense for Intelligence and Security
At the United States Senate Select Committee on Intelligence
July 10, 2024

(As of 1700 07/08/2024)

DoD also has new leadership and experts in key positions responsible for NBIS development. Along with Director Cattler, DoD brought in both a new Program Executive Officer and a new NBIS Program Manager. The new Program Manager joins us with a wealth of expertise and experience in delivering through Agile methodologies—something lacking in past NBIS program management. We have also enlisted expertise from the Defense Digital Services under our Chief Digital and Artificial Intelligence Office. Dr. Plumb will testify today to DDS's focus on modular data architecture, building the right teams, and adopting digital transformation best practices, all of which will be instrumental in strengthening the NBIS program.

Combined with improved oversight, new leadership, and greater technical expertise, we are moving forward with several initiatives. The program is fully focused on Agile software development with strong involvement from our users to ensure timely feedback and value assessments of product deliveries. To support this, we are updating foundational documentation to clearly outline roles and responsibilities, establishing the program's core capability requirements in support of Trusted Workforce 2.0, and driving improvements across the board. These efforts will result in more robust, transparent, and reliable cost, schedule, and performance metrics, improving trust in future delivery of capabilities. Recovery is not quick. This will be a month's long exercise to build a foundation enabling the Department to deliver NBIS.

Despite the issues, the Department has successfully enrolled its entire national security population into Continuous Vetting, or CV. CV is an effective model that relies on automated record checks and the reporting of relevant information from Components to enable the near-real time identification of risk. Our data indicates we are identifying potentially concerning behavior significantly sooner than traditional periodic reinvestigations. This early detection enables a strengthened security posture, supporting our critical missions across the Department. Additionally, within the Department, Trusted Workforce 2.0 policies are driving robust information-sharing between our agency insider threat hubs and the personnel vetting enterprise, allowing us to better identify and mitigate potential risks.

In closing, the Department of Defense remains committed to the NBIS program and providing secure and effective personnel vetting processes, services, and systems so that government agencies and members of our Nation's industrial base have confidence in their trusted workforce. While we cannot undo the missteps of the past, I am confident that we are on the path to success for NBIS. It is of paramount importance that the Department regains and maintains the trust of Congress in these efforts if we are to maintain strategic advantage over our adversaries. I thank the members of this Committee for your strong support of the Department of Defense, and I look forward to answering your questions.

Chairman WARNER. I would urge everybody to please stick to the three minutes that we were promised on your openings.

Just to make clear for all of those who are interested, this is not an intelligence failure, it is not DCSA, it is not NBIS. The Senate Recording Studio owns the microphones, and something I guess right before the hearing started, they got fried. That doesn't mean that the Chinese are not culpable, but we don't have direct proof on that yet.

Vice Chairman RUBIO. Until proven otherwise.

Chairman WARNER. I think, Mr. Cattler, you're up next, right?

STATEMENT OF DAVID CATTLER, DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Director CATTLER. Chairman Warner, Vice Chairman Rubio and distinguished Members of the Committee, I'm honored and grateful for the privilege to testify before you today. Thank you for the attention you're giving to Trusted Workforce 2.0 and to the National Background Investigation Services Program. I will act with the same urgency to ensure that DCSA is responsible and accountable in both what we say and what we deliver.

DCSA provides integrated security services that protect America's Trusted Workforce and cleared workspaces. We are the Federal Government's largest investigative service provider and provide vetting services for 95 percent of the Federal Government. Last year, DCSA's personal security team conducted 2.7 million investigations, 668,000 adjudications, and performed the continuous vetting of over 3.8 million people in the Trusted Workforce.

DCSA is also the primary implementer of the Trusted Workforce 2.0 initiative. Our NBIS program supports this reform effort as a federal IT system for end-to-end personnel vetting. We have faced challenges delivering NBIS to meet the expected timelines for Trusted Workforce 2.0 implementation. NBIS is unacceptably delayed and has cost far more than anticipated.

Internal and external assessments of the NBIS program identified key problems across a variety of aspects, including oversight, program management, software development methodologies, acquisition strategy, team competencies, and leadership. As Under Secretary Harris indicated, the Department's 90-day sprint effort has focused efforts on understanding and addressing these issues.

One of the outcomes of this effort is an initial 18-month capability roadmap for NBIS development. It addresses the Trusted Workforce 2.0 technical requirements and also secures requirement alignment across the DOD. We have a plan, but we are not yet recovered. Our plan is not yet approved by our DOD Acquisition Decision Authority, and once approved, we will need time to execute the plan. To be clear, NBIS development then will extend beyond the next 18 months, but I'm confident in this path to reset the program and also in DCSA's internal actions to support NBIS recovery and to improve our visibility and management of the program itself.

Also, as Under Secretary Harris noted, DCSA has onboarded new NBIS leadership to develop and implement this new roadmap. This leadership team has also evaluated and aligned a disciplined contracting strategy to support this way forward. We will obtain a new

independent cost estimate to assist with developing a reliable funding profile for the program.

In the meantime, we are committed to funding additional NBIS development without passing the costs on to our customers. We are working with our DOD partners and with OMB on funding options. We continue to engage customers and partners to ensure their feedback is incorporated as we implement this new roadmap. We will continue to address the GAO recommendations, as well.

I have also directed our DCSA Inspector General to audit the NBIS program to ensure internal accountability for both the past and moving forward. We will move forward at a responsible pace to ensure that we understand the problems and are addressing them.

So, in conclusion, we will move forward with a program that instills confidence, a program that delivers and upholds this mission without fail. We've embraced collaboration with our oversight partners and with our mission owners. Together, we will put NBIS on a sustainable pathway forward to ensure a trusted workforce to protect the Nation and secure the public's trust.

I'm confident in our path forward and do expect to be held accountable for our performance. Thank you.

Dr. Plumb will now testify to DDS's focus on modular data architecture, building the right teams and adopting digital transformation best practices.

[The prepared statement of the witness follows:]

Personnel Vetting, Security Clearance Reform, and Trusted Workforce 2.0

Statement for the Record

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Mr. David Cattler, Director

10 July 2024

Introduction

Chairman Warner, Vice Chairman Rubio, and distinguished members of the Committee. My name is David Cattler, and I joined the Defense Counterintelligence and Security Agency (DCSA) as Director in March 2024. From my first day as Director, I was humbled by the hard work and dedication of the women and men at DCSA who dutifully support key security functions across the entire Federal government. There was a lot to learn about DCSA as it is an agency with multiple missions—personnel vetting, industrial security, counterintelligence, insider threat, and security training.

I appreciate this opportunity to testify before you at this hearing. I am honored to testify alongside the Undersecretary of Defense for Intelligence and Security, the Honorable Milancy Harris, the Principal Deputy Director of National Intelligence, the Honorable Stacey Dixon, and the Department's Chief Digital and Artificial Intelligence Officer, Dr. Radha Plumb. Thank you for your oversight, the urgency you have afforded it, and the attention to the Trusted Workforce 2.0 and the National Background Investigation Services (NBIS) program. I will act with the same urgency to ensure DCSA is responsible and accountable in what we say and deliver.

DCSA's shortcomings will be set right under my direction. I welcome and am grateful for the assistance and technical expertise offered by our oversight partners and DoD stakeholders, and I expect to be held accountable.

The Role of DCSA and NBIS in Trusted Workforce 2.0

DCSA is the Federal government's largest investigative service provider, providing vetting services for a total of 95% of the Federal government. DCSA is the primary implementor of the Trusted Workforce 2.0 (TW 2.0) personnel vetting reforms. Last year, DCSA's Personnel Vetting mission conducted 2.7 million investigations, 10,700 investigations per day, 668,000 adjudicative decisions, and the continuous vetting (CV) of over 3.8 million people in the trusted workforce.

The TW 2.0 initiative is a whole-of-government effort led by the Performance Accountability Council (PAC) to overhaul the personnel vetting process for security, suitability, and credentialing. This modernization of the vetting model is a fundamental shift to improve efficiencies and the effectiveness of our personnel vetting processes, enable workforce mobility throughout the Federal government, and facilitate interagency information sharing.

The Department's NBIS program supports the TW 2.0 reform effort as a Federal IT system for end-to-end personnel vetting — from initiation and application to background investigation and adjudication, to Continuous Vetting. NBIS will deliver robust data security, enhance customer experience, and integrate data access across the whole of government and cleared industry. NBIS will provide the IT system needed to ensure a trusted workforce for 115 Federal agencies, including the DoD, and over 13,000 cleared industry organizations with contractors working for or on behalf of the Federal government.

NBIS Development

In 2015, the Office of Personnel Management announced their background investigation system had been severely compromised. The President issued Executive Order (EO) 13467, which *inter alia* tasked the Secretary of Defense to develop a modern and secure replacement IT system to support the end-to-end vetting processes for the DoD and Federal government customers. DoD's NBIS program was established in 2016 at the Defense Information Systems Agency (DISA) to replace OPM's legacy background investigation IT systems.

In 2020, a year after the agency was formed, the NBIS program was transferred to DCSA. At the time of transfer, only one NBIS capability had been delivered and put into use by DoD and other Federal agencies. This capability, called the Position Designation Tool, continues to be used to standardize position designations and inform vetting requirements. DCSA upgraded and hardened the legacy background investigation IT systems the NBIS program was established to replace, and they are still in use today to deliver vetting services as NBIS development continues. DCSA is responsible for maintaining these legacy systems until they are subsumed into NBIS.

Last year, we discovered several issues with the NBIS program after an internal DCSA assessment, the preliminary findings of a General Accountability Office (GAO) report released in August 2023, and reviews led by the Office of Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). These reviews determined there will be a delay in NBIS delivery and sunsetting of legacy IT systems, hindering the timely achievement of critical TW 2.0 milestones and the Federal government's implementation vetting reform. The analysis of the NBIS program identified several key problems including in oversight, software development methodologies, acquisition strategy, team competencies, and leadership:

- A shortage of critical technical, agile, acquisition, and integration skills hindered DCSA's ability to lead and implement a program of this scope and complexity,

- The NBIS program did not maintain an accurate integrated master schedule and lifecycle cost estimate based on requirements that were provided to the program. As TW 2.0 policy evolved, the lack of adherence to a rigorous requirements management process resulted in requirement changes and program actions. DCSA was unable to accurately assess or report on the cost, schedule, and performance impacts to inform decision-making about the program.
- DCSA measured success based on software code releases that did not aggregate to a usable capability, resulting in significantly underestimating the timelines to deliver services to our DoD and Federal customers.
- The decision in October 2020 to transfer the management of legacy Information Technology systems to DCSA, resulted in a shift in focus towards addressing cyber security standards and compliance without additional personnel or resources to perform these duties. The cost, schedule, and performance impacts of these additional responsibilities were not assessed or reported.

DoD 90-day NBIS Recovery Plan and Immediate Actions

When I began as DCSA's Director on March 24, 2024, the OUSD(I&S) had finalized the plans to begin a 90-day NBIS sprint effort to understand and address the acquisition approach, financial status, technology approach, and requirements governance in partnership with our DoD colleagues—the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), the Chief Digital and Artificial Intelligence Officer, and other Department experts. The Department's holistic approach looked at multiple facets and interdependencies of the program. The Department began that effort on 1 April, and we have worked together closely throughout the process.

Upon approval from the Acquisition Milestone Decision Authority, USD(A&S), key outcomes from the recovery plan will include the baseline and alignment of resources around clearly defined requirements, the delivery of a capability roadmap for internal and external planning and programming, the stand-up of a new NBIS leadership team with clear roles and responsibilities, a disciplined contracting strategy, and the establishment of a reliable funding profile to stabilize and sustain the program.

The OUSD(I&S), as the Program Sponsor for NBIS, will drive collaboration across the Department and lead a new NBIS requirements process. This will improve requirements management and allow DCSA to sharpen its focus on NBIS delivery. As Program Sponsor, OUSD (I&S) is updating the Capability Needs Statement and the User Agreement, two foundational documents that define the program and drive requirements and user governance.

DoD transferred the NBIS Milestone Decision Authority from DCSA to the USD(A&S) for acquisition oversight. We are moving through the stages of the approval process, which will culminate in an in-progress review meeting in early July. The elevation of oversight adds rigor and discipline to the acquisition process necessary to guide a major program of NBIS' size through the software acquisition pathway.

OUSD(I&S) and DCSA have together hired new leadership. In addition to my appointment as Director on 24 March, DCSA has upskilled the NBIS team by hiring a highly experienced and knowledgeable NBIS Executive Program Manager (EPM) and Program Executive Officer (PEO) to lead and supervise the program.

Working with this new team, I directed an internal NBIS program restructuring to comply with proper governance, business, and security protocols. We are also strengthening NBIS cybersecurity as recommended in a recent GAO cybersecurity report. We continue to work in partnership with the Defense Digital Service to focus on human-centered design and understanding the user experience to inform our modernization activities.

In order to aid my strategic guidance and to ensure internal accountability, I have also directed our DCSA Inspector General (IG) to audit the NBIS program to assess whether and to what extent: 1) funding was expended, and capabilities were delivered to functional and end users; 2) quality metrics exist, and if so, whether they are accurately measured and reported; and 3) internal controls are in place, appropriately designed, and operating effectively to provide reasonable assurance that the performance objectives of the program are being achieved. The DCSA IG will collect all historical documentation to support his assessment with a focus on FY21 to FY24. I will ensure he has the full cooperation of the DCSA workforce and full access to DCSA records.

Way Forward on NBIS

DCSA will prioritize five actions over the next 18 months: modernizing and migrating NBIS applications, aligning acquisition and development actions, adapting our NBIS workforce, aligning program cost and service pricing, and strengthening cybersecurity protections.

First, we will conduct a wholesale digital transformation to implement the proposed capabilities in the NBIS capability roadmap over the next 18 months. Subject to approval by our Acquisition Decision Authority, I will put in motion the migration of select systems to the DoD Joint Warfighting Cloud Capability (JWCC). This will give NBIS a stable, modern platform, security, the ability to scale and will

provide application developers and investigative service providers access to modernize to their specific needs. In time, this move will allow for shared services. The proposed 18-month NBIS capability roadmap includes milestones of ongoing product delivery and support to the mission owners, and the underlying data and engineering elements required to effectively operationalize capabilities in the cloud.

Second, we will assess, review, initiate technical and contractual actions to support the implementation of the NBIS capability roadmap in an 18-month timeframe in close coordination and subject to approval by our oversight authority.

Third, we will implement the recommendations of a manpower skill review to include targeted hiring, internal restructuring, and training of our NBIS team to ensure we have the required deep technical expertise and senior acquisition expertise required for a program of this magnitude and complexity.

Fourth, I am working with my Chief Financial Officer, the OUSD(I&S), the DoD Comptroller and OMB to assess cost and pricing impacts due to the delay in NBIS deployment to develop courses of action to minimize the impact to our customers. The milestones in the NBIS capability roadmap will drive the costs and impact. DCSA will communicate any potential impact of product and service rates charged to our customers. Aligned with prior year practices, the Department announced preliminary FY26 rates at the Enterprise Investment Board meeting on June 27, 2024, and will set final rates for FY26 in August 2024.

Finally, we continue to work closely with GAO on ongoing assessments. The team is actively addressing process and satisfying administrative deficiencies that were identified in a forthcoming GAO report on cybersecurity compliance. I have prioritized these efforts and have instructed my teams to fully integrate cybersecurity oversight and governance of NBIS with DCSA Chief Information Officer and the Chief Information Security Officer.

TW 2.0 Is Being Successfully Implemented

Before closing, I want to share several major TW 2.0 milestones that DCSA has helped the DoD and federal agencies implement to improve efficiencies and reduce risk in the trusted workforce to include deploying case initiation capabilities for DCSA customer agencies and industry to initiate vetting within NBIS, establishing and delivering Continuous Vetting services for DCSA customers, and improving reciprocity timeliness.

- Transition from e-QIP to eApp. All 115 customer agencies and more than 10,000 industry companies have been onboarded into the front end of NBIS. This allows these entities to initiate cases in NBIS

and for applicants to use the Electronic Application (eApp) to complete their vetting forms, replacing the previous application, Electronic Questionnaires for Investigative Processing (e-QIP) and improving the applicant experience.

- Tool to standardize position designation decisions. The Position Designation Tool, mentioned earlier, is used by all Federal agencies to assign position sensitivity and risk determinations. The tool helps ensure positions are properly designated to protect national security, public trust, and the integrity of government operations and establishes consistency across all agencies for the level of investigation needed for that position.
- Rapid reciprocity decisions to increase workforce mobility. Reciprocity timeliness remains at all-time lows for transfers into DoD. Through process improvements, we reduced the time to make a reciprocity decision into DoD to an average of one day, down from 65 days in mid-2020.Continuous Vetting serves to replace periodic reviews. Our Continuous Vetting services are being used across the DoD and more than 90 non-DoD entities, enrolling more than 3.8 million personnel. The program is preparing to expand to wider Federal populations this summer. Continuous Vetting enables DCSA to identify and mitigate risk in the trusted workforce in a matter of days and weeks, rather than years under the periodic reinvestigation construct.

The TW 2.0 Continuous Vetting model, especially, delivers a comprehensive and efficient vetting process, helping risk management decision-making by focusing in-depth investigations on specific issues of greatest concern. Continuous Vetting involves regularly reviewing an individual's background through automated records checks, time or event-driven investigative activity, and information such as self or command reporting, security incidents and violations, and insider threat information. The implementation of Continuous Vetting has been crucial in ensuring that the personnel vetting process continues to make improvements in security, quality, and efficiency.

In addition to the success of Continuous Vetting, the fastest 90% of end-to-end timeliness of DCSA-provided background investigations has gone from over 400 days for a top-secret investigation in April 2018 to an average of 187 days in May 2024. This current average is up by 80 days from its lowest point in FY2021, due to a recent surge in demand for background investigations. Through a combination of process improvements, technology adoption, and an increase in workforce size, DCSA and its predecessor agencies were successful in reducing the amount of time it takes to process a clearance, getting trusted personnel to work more quickly in critical positions. Reductions of timelines allow our government employees to commence work more quickly, ensuring that key talent is in place to fill important national security positions, while meeting the needs of the American people.

Continued implementation of TW 2.0 will further improve efficiencies in the personnel vetting process. TW 2.0 brings new data sources, new timeliness standards, and new enterprise tools such as the Personnel Vetting Questionnaire and self-reporting. With the aid of full NBIS delivery, the Federal government will see improved information sharing, and a risk-based trusted person model.

Conclusion

The Executive Branch and Congress have entrusted DCSA with delivering NBIS to enable full implementation of TW 2.0. When deployed, NBIS will support the personnel vetting mission and our customers who utilize NBIS for its secure and efficient investigation and adjudication process. DCSA and the DoD are committed to its development and fielding, and we will finish our part.

DCSA has several steady partners in examining NBIS and identifying the many challenges it faces. We are systematically addressing these issues raised by our partners and taking bold action to correct deficiencies as identified during our 90-day recovery plan. We've taken these lessons learned seriously and to task. DCSA will move forward with a program that instills confidence; a program that delivers capabilities to uphold mission without fail. I am confident in our path forward and expect to be held accountable. We've embraced collaboration with our oversight partners, GAO, DoD, the PAC members, and mission owners—together we will take NBIS on a sustainable pathway forward to ensure a trusted workforce, to protect the Nation and earn and secure the public's trust.

STATEMENT OF RADHA PLUMB, PH.D., CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER, U.S. DEPARTMENT OF DEFENSE

Dr. PLUMB. Chairman Warner, Vice Chairman Rubio, and distinguished Members of the Committee: I appreciate the opportunity to testify here before you today on the chief digital and artificial intelligence officer role in the NBIS recovery efforts.

Our CDAO team has partnered with our colleagues across the Department of Defense through a 90-day discovery sprint. We focused on characterizing the problem space, user needs, as well as mission and technical requirements. We then work with partners across DOD to ensure any proposed technology changes align to the full set of requirements for NBIS.

As we've seen in other enterprise level implementation issues across DOD with analogous examples in the private industry, modernizing and scaling a technical capability requires both change in the underlying technology and a change in mindset and culture.

The CDAO has made a number of specific recommendations to DCSA related to the technical NBIS solution, which can be grouped in three big areas. The first group relates to technical approach to delivering a modular data architecture. The second group focuses on building the right teams and aligning those teams on products rather than features and capabilities. And the third area focuses on adopting digital transformation best practices. The overall technical approach we recommend is to build upon the existing systems where possible, and build the digital solutions needed in targeted areas where needed. This, combined with the expansion of technical talent and the adoption of Agile software development methodologies provides a robust framework for success.

I'll close by noting that in addition to the shift in technical approach, we need a mindset shift. Unlike hardware procurement, software delivery never reaches a discrete endpoint for both the front and back-end system development. We should anticipate needing to devote time and resources to continuous development cycles that will maintain and continuously improve the technology.

Thank you. I'll now turn over to Honorable Stacey Dixon to discuss the implementation of the Trusted Workforce 2.0.

[The prepared statement of the witness follows:]

STATEMENT BY

DR. RADHA IYENGAR PLUMB

DEPARTMENT OF DEFENSE
CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER

BEFORE THE

SENATE SELECT COMMITTEE ON INTELLIGENCE

ON

NATIONAL BACKGROUND INVESTIGATION SYSTEM AND OTHER MATTERS RELATED TO TRUSTED WORKFORCE 2.0 AND PERSONNEL VETTING

JULY 10, 2024

Chairman Warner, Vice Chairman Rubio, and distinguished members of the Committee, I appreciate the opportunity to testify before you today on the National Background Investigation Services, or NBIS, program, and our efforts to support a modern, end-to-end personnel vetting process.

As you heard from the other witnesses, the Chief Digital and Artificial Intelligence Office has partnered with our colleagues across the Department of Defense (DoD) to realign NBIS governance and development processes through the Defense Counterintelligence and Security Agency (DCSA) 90-day Recovery Plan.

In February 2024, the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) requested the Chief Digital and Artificial Intelligence Office (CDAO) and its Defense Digital Service (DDS) to perform a technical assessment of NBIS.

To formulate recommendations, we conducted a 90-day discovery initiative, in close cooperation with DCSA. During this process, the CDAO team learned about the overall problem space, user needs, as well as mission and technical requirements. We then worked with partners across DoD to ensure any proposed technology changes aligned to the full set of requirements for NBIS.

As we've seen in other enterprise-level implementations within DoD and with analogous examples in private industry, modernizing and scaling a technical capability doesn't just require a change to the underlying technologies but also a change in mindset and culture. For that reason, our recommendations highlight both the "what" (i.e., the technology) and the "how" (i.e., the people and processes).

CDAO made a number of specific recommendations to help DCSA deliver a technical NBIS solution that meets the needs of DoD and the federal government. These include:

1. Data Architecture: Rather than treat NBIS as a single, monolithic system, we believe the best approach going forward is to maintain a modular architecture to enable flexibility and adaptability for future changes. That modularity allows NBIS to leverage existing applications that are working well today and focus resources on addressing other components with the greatest technical risk.

To drive down technical risk, we recommend migrating to more modern and reliable compute and storage infrastructure using modern software engineering approaches. This then allows NBIS to achieve modularity more rapidly by investing in Application Program Interfaces (APIs). These essentially create common connectors between different components.

This process to connect different components will also rely on identifying and consolidating data sources, developing data standards, and deduplicating data where it exists, with the ultimate goal of having a shared data service.

2. Build the Right Teams: CDAO and our DDS team believe having the right people, with the right skillsets, is critical to delivering on our technical recommendations.

In particular, this includes a team developing a BI application using Trusted Workforce 2.0 as a first principle and ensuring an appropriate government and contractor workforce with technical skills, data and IP rights management, and API interface design and maintenance.

This also includes integrating product trios of product manager, user experience/research & design, and engineer, and aligning teams on products rather than features or capabilities.

3. Adopt digital transformation best practices: It is essential to recognize the unique challenges of conducting agile software development within the government sector. Agile methodologies, which emphasize iterative progress, flexibility, and customer collaboration, can often conflict with perdurable government processes and deep-seated culture.

This includes adopting an agile and customer-first mindset across all organizational levels to foster a cohesive, responsive, and efficient working environment. To support that, we should align requirements gathering to User-Centered Design and Agile software development within the NBIS Program Office and ensure the Authorizing Official (AO) responsible for cybersecurity follows an approach that affords iteration while maintaining compliance.

Leveraging the elevated requirements and acquisition processes, we believe these technical recommendations enable the NBIS program to significantly improve its system architecture, organizational structure, and user experience, ultimately ensuring a more secure and efficient background investigation process for DoD and the federal government.

While the path to modernizing our personnel vetting systems faces challenges, the strategic decision to build upon existing systems, combined with the expansion of technical talent and the adoption of agile methodologies, provides a robust framework for success. With these measures in place, NBIS is well-positioned to enhance the efficiency, security, and effectiveness of our personnel vetting processes, ultimately strengthening our overall national security infrastructure.

Lastly, and perhaps most important, we need to acknowledge that software delivery never reaches a discrete endpoint. Unlike hardware procurement, we should anticipate to always devote time and resources to maintaining and improving the technology. This is a mindset shift that needs to be applied to NBIS.

CDAO looks forward to continuing to work with DCSA in designing, developing, and deploying a viable, desirable, feasible, and usable NBIS program.

Thank you to the members of this Committee for your ongoing support and collaboration, and I look forward to answering your questions.

STATEMENT OF STACEY DIXON, PH.D., PRINCIPAL DEPUTY DIRECTOR, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Director DIXON. Chairman Warner, Vice Chairman Rubio, Members of the Committee, thank you for the opportunity to appear before you today to discuss personnel vetting reform.

I am pleased to represent the Director of National Intelligence, Avril Haines, who serves as the security executive agent for the Federal Government. In this role and as head of the Intelligence Community, she develops and oversees policies and standards for determining an individual's eligibility for access to classified information and to occupy a national security or sensitive position.

Trusted Workforce 2.0 helps us ensure vetting processes are effective, timely, fair, and secure. It is centered around a risk-based model that leverages modern IT, improves timeliness, reduces complexity, and eliminates repetitive and duplicative investigative actions. Doing so improves the mobility of the workforce to respond to mission needs and helps us detect and mitigate risk earlier.

We've established a more consistent vetting foundation by creating guidelines and standards that identify intended outcomes for personnel vetting. Despite many achievements, much work remains. Implementing the most aggressive security clearance reform in decades takes time. The Honorable Harris, the other PAC principals at OMB and OPM, and I work diligently to address clearance reform challenges in an intentional way, taking into account views from multiple partners, to include Congress.

We acknowledge there are still areas where we must together plan for how best to achieve success. Reciprocity and the broader transfer of trust is one such area. The security portion of reciprocal determinations continues to improve, with most agencies completing that determination within five days. Nevertheless, other transfers of trust take more time as one would expect. Factors such as polygraph requirements, medical evaluations, new continuous vetting alerts or the new job requiring different kinds of access to sensitive information may also increase the time it takes to move individuals from one agency to another.

There's also an increased demand for expanded transparency between agencies related to personnel mobility. To address this challenge, we're developing software that will provide greater visibility for the gaining agency, so they have direct access to information they need to make transfer of trust determinations.

Measuring the success of Trusted Workforce 2.0 is also important. Therefore, we're working to create a more automated solution to assist agencies in reporting their metrics.

In closing, we believe it is imperative we stay focused on improving and completing implementation of the Trusted Workforce 2.0 transformation. The success of this personnel vetting reform effort will continue to require strong senior leadership commitment as well as Congressional support.

Thank you for the opportunity to testify before you today. We look forward to your questions.

[The prepared statement of the witness follows:]

Statement for the Record
The Honorable Stacey A. Dixon, Ph.D.
Principal Deputy Director of National Intelligence

Hearing on NBIS and Personnel Vetting Reform
Senate Select Committee on Intelligence

Wednesday, July 10, 2024

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for the opportunity to appear before you today to discuss personnel vetting reform milestones achieved to date as well as the next steps moving forward.

I am pleased to be here representing Director of National Intelligence (DNI) Avril Haines, who serves as the Security Executive Agent for the Federal Government. As the Security Executive Agent and head of the Intelligence Community, the DNI develops and oversees policies and standards for determining an individual's eligibility for access to classified information or to hold a sensitive position. Her responsibilities include developing and issuing uniform and consistent policies and procedures, along with exercising oversight, to ensure that these vetting processes are effective, efficient, timely, fair and secure.

Since I last spoke before this committee on the topic of personnel vetting reform in March of 2023, implementation of Trusted Workforce 2.0 has continued to mature and have a positive impact on our entire Federal Workforce.

The current Trusted Workforce 2.0 effort is transformative – it is centered around a risk-based model that leverages modern IT, improves timeliness of personnel vetting, reduces complexity, and eliminates repetitive and duplicative investigative actions. By making personnel vetting processes more consistent across the government enterprise, leveraging technology and automation, and shifting away from the traditional periodic reinvestigation model, Trusted Workforce 2.0 seeks to deliver talent to the mission faster. Doing so improves mobility of the workforce to respond to mission needs and aids the ability to detect and mitigate risk earlier.

Through the issuance of several policy documents, we have established a more consistent vetting foundation by creating guidelines and standards that identify intended outcomes for personnel vetting. We have created an engagement approach that emphasizes trust in the process and shapes a culture of personal accountability and shared responsibility between the individual being vetted and the personnel vetting practitioners. We have revised the investigative standards and issued new performance management standards to ensure that personnel vetting practitioners are satisfying goals and measures in line with expected outcomes of Trusted Workforce 2.0.

Agencies have identified Trusted Workforce 2.0 Senior Implementation Officials and our teams work very closely together to ensure implementation of these policies is progressing effectively.

Based on extensive feedback from personnel vetting practitioners, agencies, and the public, we have modernized the Personnel Vetting Questionnaire (PVQ) to improve our ability to collect information more comprehensively and aligned with the revised investigative standards.

We have successfully implemented the continuous vetting capability for our National Security population that allows the receipt of information in near real time. Data generated through a combination of ongoing automated record checks, user activity monitoring, adjudicatively relevant insider threat information, self-reporting and agency specific information creates the ability to respond to issues much more quickly.

Not only does Continuous Vetting improve the protection of IT systems, facilities, people and mission, it also introduces a robust wellness factor by allowing earlier identification of problems such as financial hardships, substance abuse, and addictive behaviors, as reflected in collected information. By identifying these issues more quickly, agencies are able to intervene earlier and leverage available resources within the government to provide the assistance employees need.

We are now looking to expand the continuous vetting capability to the Non-Sensitive Public Trust (NSPT) population. This effort will ensure the delivery of a trusted workforce beyond just the National Security population.

Despite all of these achievements, much work remains to be done. Implementing the most aggressive clearance reform effort in decades has taken longer than we had hoped. The important thing is that we get this right and maintain the right balance between delivering a trusted workforce and managing risk.

Streamlining reciprocity and the broader transfer of trust are examples where work continues. Improved personnel mobility across the enterprise is a major goal of this effort. Reciprocal determinations from a security perspective continue to improve with most agencies completing that determination within five days. This is evidence that a Top Secret clearance sponsored by one agency is accepted by a gaining agency without additional vetting. Despite these favorable statistics for reciprocal determinations made by personnel vetting practitioners, the actual transfer of trust from one agency to another takes more time, as would be expected. Factors such as polygraph requirements, medical evaluations, access to more sensitive information or more restricted IT networks, and continuous vetting alerts may increase the time it takes to move individuals from one agency to another, especially within the Intelligence Community.

Another rising issue related to personnel mobility is transparency. Favorable Transfer of Trust and reciprocity determinations are achieved based on the gaining agency accepting the prior vetting of an individual. Previously, the date of an individual's background investigation was a factor in that determination. As we pivot to continuous vetting and eliminate the common

practice of confirming the date of a reinvestigation, we are receiving a demand signal from gaining agencies who are requesting more transparency into actionable CV alerts, previously submitted information collection forms, HR related actions such as medical evaluations, and self-reported activities.

In response to the increased demand for expanded transparency between agencies related to personnel mobility, we are working to deliver a high side Information Technology (IT) solution that will provide greater visibility into the information needed by the gaining agency. The Transparency of Reciprocity Information System (ToRIS) will allow agencies access to required information on an as needed basis with the intent to enhance Transfer of Trust determinations.

ToRIS is not duplicative of NBIS, and will leverage some NBIS capabilities such as the electronic application (eAPP) function, allowing applicants to submit their required paperwork in eAPP and then have an IC element transport that information to the high side for processing.

Regarding hiring timelines, within the Intelligence Community, we are seeing an overall improvement. In parallel to Trusted Workforce 2.0 implementation, the ODNI has been driving a 180-day hiring timeline initiative. This initiative requires IC Elements to streamline efforts and improve efficiencies in each facet of the hiring process. The Performance Management Standards are looking to further decrease that hiring timeline to an aspirational 130 days within the next four years, as we agreed to during the March 2023 Personnel Vetting hearing.

Measuring the success of the Trusted Workforce 2.0 effort is imperative. Embedded within the ODNI National Counterintelligence and Security Center is a metrics collection team who gathers data from across the Federal Government to assess the performance of agencies' personnel security vetting programs, to include timeliness. This team is working to create a more robust template aligned to the recently issued Federal Personnel Vetting Performance Management Implementation Guidance (PMIG). This new template will assist agencies in transitioning to the new reporting requirements of Trusted Workforce 2.0 with as little disruption as possible while, at the same time, allowing for automated data collection that can be analyzed more effectively.

In order to enhance this automated process, we are working to deliver an IT capability called Security Metrics and Quality Reporting Tool (SMART), which reimagines how customers interact with personnel vetting performance data. SMART will simplify data management, foster greater collaboration among users, and ensure robust data protection measures for enhanced security. SMART-provided indicators and measures will not only provide the information oversight entities require to ensure the success of the Trusted Workforce 2.0, but will give agencies the insights they need to sustain healthy personnel security vetting programs that promise a trusted workforce across government.

Along with my colleagues here alongside me, as well as with PAC Principals, OMB and OPM, we are working collaboratively to address gaps in the clearance reform effort as Department and Agencies continue to work through their implementation strategies and initiatives.

My colleagues and I work with and take into account views from multiple partners including interagency security personnel, civil liberties and privacy experts, legal advisors, hiring officials, industry partners, and Congressional Committees.

I would like to particularly emphasize the important role that our industry partners play as they have been instrumental in our ability to make sustained progress. We have intentionally increased our engagement and outreach with industry representatives. Their voice and advocacy for transformation has tremendously assisted the Trusted Workforce 2.0 team in identifying challenges and addressing their concerns. As an example of this collaboration, the ODNI is working to promote enhanced information sharing and facilitate clearances for companies' key management personnel. These are both issues previously raised by this committee.

In closing, we believe it is imperative to stay focused on improving and completing implementation of the Trusted Workforce 2.0 transformation. The success of this personnel vetting reform effort will continue to require strong senior leadership commitment and support from Congressional leaders such as yourselves.

Thank you for this opportunity to testify before you today – we look forward to addressing any questions you may have.

Chairman WARNER. All right, Senator Rounds, what do you have to say for yourself? [Laughter]

No, no, no, you're not up on the panel.

So, you know, there's some really tough questions that need to be asked. But let me make clear, while Deputy Director Dixon has been on the PAC, the oversight board, she was not directly responsible for some of the details of some of this, although I will ask why the PAC didn't catch it.

Dr. Plumb has been brought in as one of the experts to help us figure it out. And you know, Mr. Cattler and Secretary Harris were not there when the screw ups took place. So, while I'm going to be very tough on them, my hope is that we can get some answers. But I want to make clear that for the most part, these were not the individuals, unfortunately, that were directly responsible. And I will add as well, some of the people who were responsible have almost all left the government, and they got quite an earful from me in the interim.

And just to put this, again, in a little bit of context, March of 2023, we do our normal update. We're trying to figure out—reciprocity is a huge issue. You know, you get a security clearance at DOE or DHS. Even when you had a security clearance at DHS and you wanted to move from one DHS contract to another, you still had to go through another process. It was crazy. I remember Dan Coates, who was on this Committee for many years, when he became DNI and had to go through what took a much longer process than it should, him having had access to all of the information from this Committee. So, we've been working this process, trying to drive the wait time down, trying to make sure that a clearance wouldn't have to be redone all the time.

And you know, to try to do this where we have continuous vetting using technology—not sending retired FBI agents out to check whether somebody actually went to college X—makes sense and should bring about a more efficient system. But as we said, for a program that was supposed to be done by 2019, and you can go ahead and start the clock, I'm not going to go forever on this. This was supposed to be in 2019. And in 2023, we were led to believe that things were going along even though there had been delays. The amazing thing was, in September of '23, at NBIS there was a sudden deletion of 90 terabytes of information. That's a lot of information. Now luckily, there were some backups that were able to restore that. But we asked if you hadn't had that "holy heck!" moment, would this Committee have ever been informed of how screwed up things were?

To give a framework at DCSA 5,400 employees, roughly about 1,000 of them, almost all the time we're working on this project. The outside contractor had 1,000-plus people working on it. The contractor was to my understanding developing a program that would have never scaled to meet the needs.

How did this go on without anybody saying—of a few thousand people, contractors, and government employees saying this isn't going to work?

Now some of this is due to fixed price contracts, where I don't believe we've actually set the incentives in the right place to get a product that's deliverable. But it still begs the question of, my

gosh, if there hadn't been the misplacement of 90 terabytes of data, when would we have been informed?

Starting in about November, December, we had a series of meetings I did with others, with former Secretary Moultrie on these issues. And it went from one story to another, getting worse and worse and worse. So, we've not only wasted—we don't know for a project that was supposed to cost in total an initial estimate $700 million and we're at about $1.7 billion now and we don't even know how much it will cost to finish.

You know, for you guys who thought ACA rollout was bad, this may get close in terms of cost overruns. We need to know what the expectation would be.

And I'm going to start with Secretary Harris and David, for you to give us an update. And I appreciate the 90-day sprint. And then I am going to ask Dr. Dixon, why didn't the PAC catch this, and how do we have confidence? We can bring you guys in on a regular basis, but how are we going to have confidence that this doesn't happen again? Because end of the day, as Senator Rubio said, we've got to guard our Nation's secrets. And if we can't get people cleared and people won't come to work for the IC and we can't get them to move from our contractor community, if we can't get folks to move from one contract to another, we're not going to be as efficient as we should be.

So, Ms. Harris and Mr. Cattler, if you could talk and then Ms. Dixon, if you could answer.

Secretary HARRIS. Thank you for the question. So first and foremost, we are focused on doing this once. So, this sprint effort has been focused on diagnosing what has gone on with the program and focused on moving out on an implementation plan that leads to success. That includes, as I mentioned, new oversight authority, both for the sponsorship of the program and for the acquisition. So that will both happen at the Under Secretary level in the Pentagon. This is a cross-functional effort. DCSA needs the full team at its back.

So, we are also working on clarity on requirements and a new requirements management process. That will be in conjunction with our partners in the PAC to ensure that we understand what the system needs to deliver, how our customers are using it, and what needs to be integrated into the roadmap for future development.

We are also working on, as you referenced, this roadmap for delivery so we have some predictability, so we can measure how we are doing against those goals, and that we can better mark where we have delays or other technical problems that are interrupting the development cycle. And finally, we are working to develop a reliable funding profile aligned to that new roadmap.

As David alluded to in his statement, we are conscious that we need to, as the Department, take the costs of this delay and fund those internally. We are working through that in our current program budget review, but we are confident that we can continue to deliver this program if we align to these goals.

Chairman WARNER. Well, I would like brief answers because I'm chasing away my colleagues. But I'm going to be here as long as it takes. So, I've got lots of rounds of additional questions. But you

know, and I appreciate, Mr. Cattler, you coming in to take this on because it it's a mess and I appreciate that.

But if you could briefly—and then Secretary Dixon or Director Dixon, could you briefly, because I want to make sure everybody gets a bite.

Stacey, I'm going to save you for my second round, so you get a reprieve, but how do we make sure that we've actually got a plan and please give as much specificity as possible, but briefly. And I have lots of follow ups for later.

Director CATTLER. Well, thank you, Chairman. I'd just reinforce what the acting Under Secretary said. First by saying that I joined literally a week before that 90-day period began for the review and was able to then plug into that fully. And I'm confident that we brought the right people to bear to take a hard look at this.

From my perspective, we considered personnel—personnel expertise, as a first basket. We looked at procurement as a second and we looked at oversight as a third. And we've both made many points already, but happy to amplify on what the specifics were that we went through as we did that review.

But moving forward, we have new oversight authorities. We will have clarity on program requirements and new requirements management process. And I think it's important to say here that the Trusted Workforce requirements, as well as those in NBIS as initially conceived are understood and sound. I think the problem really was their interpretation and making sure that my agency had what it needed in terms of its knowledge and capability to actually deliver properly on those requirements. And this was a large part of this discovery process as we went through it.

We will also have an updated and good vetting capability roadmap for delivery and a reliable funding profile aligned to that new roadmap. After its approval, we will also get that outside independent cost estimate to be even more confident and in compliance with policy and the statute and be sure you have the right documents.

So, at the end of this 90 days, we will have delivered an updated set of acquisition documents. This revamped requirements governance procedures, Agile training and documentation. As Dr. Plumb has also said, we've brought in some new people. We know where our gaps are in the skill sets that we need to hire on the government side. We're working with the contractor as well on actions that need to be taken there. And we are also evaluating the requirements baseline. Sir, I have a lot to say on this point, but again in the interest of time, I'll stop.

Chairman WARNER. I'll come back around. Senator Rubio.

Vice Chairman RUBIO. So this could be to Director Dixon or Secretary Harris or both. The continuous vetting in the National Background Investigation Service is not mandatory for all the agencies and departments to use as their system under the Counterintelligence and Security Agency. This directly, I think, impacts oversight by ODNI as the security executive agent. Additionally, contractors have a real tough time being able to plan and train to these very different systems and it's not easy to track whom to contact for security clearance tracking and reciprocity.

So DCSA and NBIS systems of security clearance do not cover or support the IC. Why is that? And what is the plan going forward? In particular, what about reciprocity for employees that are moving, for example, from CIA to DIA?

Director DIXON. I will take that one, Sir.

You're absolutely right that DCSA does not cover the Intelligence Community. We have a number of agencies within our community, and we essentially allow them to determine the types of risks that they're willing to take as they're bringing on board their folks. So they do their own. Many of them do their own investigative service. They also have enhanced vetting processes, to include polygraphs, medical, some psychological screenings that DCSA does not provide. But those are what they believe they need to bring on board the kinds of folks that they need for their particular workforce. To expect DCSA to do that sort of tailoring for different agencies to deliver what they need is something that we wouldn't put on them. We believe that the agencies themselves are best positioned to bring their folks on and know what kinds of vetting they actually need to do. We are very comfortable with what DCSA does for the rest of the government, but with respect to the Intelligence Community, because it is so variable between the agencies, it's better for them to be able to actually pick their processes.

Vice Chairman RUBIO. So which agencies don't use NBIS and DCSA's CV program? Which are the agencies that do not?

Director DIXON. We have within the CV particular——

Vice Chairman RUBIO. Yes.

Director DIXON. Continuous vetting is done by everyone.

Vice Chairman RUBIO. Right.

Director DIXON. It's just done differently. We have a continuous evaluation system that we use within the Intelligence Community, but it uses many of the same reports and data sources that the CV does—it uses for DCSA. So there's commonalities there. It is just a different system that we run.

David, do you want to——?

Director CATTLER. Yes, thanks.

I'll just add from the DCSA perspective, we're managing enrollment and alert resolution for 3.8 million Department of Defense, military civilian, and National Industrial Security program contractors, but also for 44 non-DOD federal agencies. So it's a very large population that we're handling outside the IC.

Vice Chairman RUBIO. So is not having a sort of a single—or at least as a baseline—a single NBIS like system for the federal government, doesn't that hamper efforts at reform and oversight, because we're in essence dealing with all these silo type systems?

Director DIXON. Our answer actually would be no, Sir. Because Trusted Workforce 2.0 is bringing in the standardization and the guidelines, so that even though we're using different investigative processes, the underlying principles behind them are the same.

And what will happen with a clearance, the types of security clearances that are being granted, the types of vetting that's being done is similar across the board. When it comes to the IC, we just require more than some of the other government agencies and so we're handling that "more" section. So it's really the baseline and

foundation are similar. It's just the extra parts are different for what our community needs.

Vice Chairman RUBIO. Okay.

Chairman WARNER. Senator Wyden.

Senator WYDEN. Thank you. Thank you very much, Mr. Chairman. And let me say to our panel, years ago, when Senator Moran of this Committee and I started on the declassification reform issue, we learned that a staffer actually had to trek around from office to office with a blue bag waiting around for approval and I always wondered whether this took so long that the staffer had to pack a lunch because it looked like they were out there for great lengths of time. This was because Senator Moran and I found that the different systems didn't talk to each other. So we're going to start speaking English now about exactly what is at issue. Then with digital records, they just overwhelmed this broken system.

So, I had a number of conversations with Director Haines. And she said: you and Senator Moran are absolutely right, and we've got to get serious about it. And she went and gave a big speech in Texas with Senator Cornyn, who's taken a great interest in it, and she said we're going to reform it.

So, I want to ask some questions now of you, Dr. Dixon, to pick up where we left off on this kind of setting-the-table that I have done here.

You were last in our hearing last March, and I asked then and I'm going to ask now: Has any progress been made in the Administration's rewrite of the Executive Order governing classification and declassification?

Director DIXON. The Administration continues to make progress on that. I believe that they will have some upcoming deliverables over the course of the summer that we're all looking forward to. But it's been a very collaborative process across the interagency, making sure that everyone's equities are being taken into account.

Senator WYDEN. So you expect that we'll get that this summer?

Director DIXON. I believe that is their goal.

Senator WYDEN. Okay. Now obviously, real reform means you got to have somebody in charge. Is the Administration any closer to designating an executive agent for classification and declassification?

Director DIXON. I would say part of the Executive Order conversations that they're having involve who that executive agent will be for declassification.

Senator WYDEN. So, will we be close to actually getting an executive agent for classification and declassification, in your view, by fall? That's a "yes or no" answer.

Director DIXON. I'm not in charge of the process. Their goal is to deliver——

Senator WYDEN. Who is? Who is?

Director DIXON. The Administration itself is actually delivering the Executive Order update. And once they deliver that, part of that is a description of who will be the declassification executive agent. Once that is defined, they will then go about filling the process.

Senator WYDEN. So when do you believe we'll have an executive agent for classification and declassification? Because that's key.

You know, in other words, Senator Warner, Senator Rubio are talking about all kinds of very serious things. And I think back through some of what Senator Moran and I have been through and the first thing we got to do is figure out how to put this in terms people can understand. The system we found with the person and his blue bag made a mockery out of what government is supposed to be all about.

I'm at the point, I'm now, I believe, the longest-serving member of this Committee. I think we're at the point where the classification system is so broken, we can't even necessarily figure out who the bad guys are and who the good guys are. So I hope you'll take back—and I'm going to be on the phone with Director Haines very quickly on this question of when we're going to get an executive agent for classification and declassification.

Director DIXON. In the meantime, Sir, we're also making some strides to actually improve declassification. But I do believe once the EO—the Executive Order is delivered, it will explain who the Executive Order agent for classification is.

Senator WYDEN. Okay. So one last question. My time is short. For you, Ms. Dixon.

So I think it is generally believed that declassification reform is going to save taxpayers some money in the long term. But we're going to have to have some investments in order to modernize the current obsolete system. Has the ODNI arrived at some estimates for how much declassification reform will cost in the next few years? A. And B, will you make public what those estimates are?

Because we have spent so much money on this, I think people have a right to know what's the answer to that. And I guess I got eight seconds to get it under the gun.

Director DIXON. With respect to the first one, we are in the process of figuring out what tools, capabilities, incentives we need to actually put in place so that people are thinking more about what information they can declassify versus how we've been protecting it in the past. I will take back whether or not we're going to be publicizing that number.

Senator WYDEN. Just know—and I'm going to say it right here. Senator Rubio, kids me from—We're going to have a real fight if there is a resistance to making those estimates public. We have spent so much money for so long. The public's got a right to know on where we go from here, especially given the fact that my Chair has asked these serious questions and we're kind of in the dark about what's happening with the delay, so that's——

Chairman WARNER. Ron, you know we had——

Senator WYDEN. Thank you.

Chairman WARNER. [continuing]. We took your and Senator Moran's bill. Senator Cornyn had a lot of work on this. We built it in. We went even further and it was all in the IAA last year. And it ended up not being this Committee; it ended up being some of our colleagues in the House. And we've still got many of those provisions in this year's IAA. So we are not letting go of that and appreciate the great work that you and Senator Moran have done. And I know Senator Cornyn has been an advocate on this as well.

Senator Cornyn, you're up.

Senator CORNYN. Well, let me start with where Senator Wyden left off, and Senator Warner. The Sensible Classification Act that we passed last year. Part of that required studies and recommendations on the necessity of security clearances.

I believe the testimony we've heard was that there are four million people with security clearances in America. If four million people are supposed to keep the Nation's secrets, it seems to me that there's a lot of not secrets being kept. I mean, that things are not secret. And we've learned that some of the FTEs require a security clearance without regard to actually the necessity of that person getting a security clearance and the like.

So what I wanted to ask is, have the agencies that you oversee begun the studies on the necessity of security clearances, including a description of how the agencies will make sure that the number of security clearances granted will be kept to a minimum?

Let me start with you, Dr. Dixon.

Director DIXON. I actually don't know the answer to that question. I will go back and find out whether the studies have begun.

Senator CORNYN. That concerns me. You're the Deputy Director of National Intelligence and you don't have that information?

Director DIXON. That particular one, no, Sir, I do not.

Senator CORNYN. Any of the rest of you have any knowledge of any studies that have been done or are in the process of being done as required by the statute?

[No response.]

Okay. Well, that's kind of not a great start.

Let me go back.

As I understand it, the Counterintelligence and Security Agency was established in 2018. Of course, the NBIS, the personnel vetting system, was supposed to be the NTI—end to end IT infrastructure to enable the comprehensive personnel vetting on a single platform. It was originally supposed to be completed by 2019—that was five years ago—at a cost of $700 million. But here we are, five years later, and the program is not operational and $850 million has been spent.

Can any of you tell us when the NBIS will become operational?

Secretary HARRIS. So we have delivered some NBIS capability to date. At this time, as part of the 90-day effort, we are re-baselining to make sure we understand exactly——

Senator CORNYN. That means you're starting over.

Secretary HARRIS. We are not starting over. As I think you've heard some of the other witnesses talk about, we're looking to make sure that we can use what has been built. We are exploring exactly what needs to happen going forward to ensure we meet the full level of capability that is expected from the system.

At this time, we are in the process of refining exactly our understanding of that timeline. I commit to this Committee——

Senator CORNYN. In other words, you can't tell us at this point.

Secretary HARRIS. I cannot tell you at this point. What I can commit to is that we will keep this Committee informed as those estimates take shape.

Senator CORNYN. Yeah.

Secretary HARRIS. We are going through the process as I discussed to work with the Under Secretary for Acquisition and

Sustainment. As part of that we are re-baselining the program. We will have an independent cost estimate. All of these are things that I commit to keeping the Committee informed on as this work takes shape.

It couldn't happen in 90 days. This is a month-long effort. But we are fully committed to making sure that you have the full visibility as it comes together.

Senator CORNYN. So you can't tell us when the NBIS will be operational at this point.

As I look at the new NBIS program manager and program executive officer has identified, it looks like four main reasons why this program is overdue and overbudget. One was the trouble with requirements. The second is too much focus on technical debt. The third is poor contract management. And the fourth is insufficient time and criteria for review. The GAO, the Government Accountability Office, has conducted multiple studies and made a variety of recommendations.

Are those recommendations being implemented in the current efforts?

Director CATTLER. Senator, yes, they are. We're taking corrective action on those. That's one commitment that I make to this Committee and to my agency.

Senator CORNYN. And who is in charge in the sense that there needs to be somebody held accountable? And as long as everybody is accountable, no one's accountable. Who is in charge of making sure this program is back on track and will be delivered as promised?

Secretary HARRIS. So, I believe that as the program sponsor, the Under Secretary for Intelligence and Security has responsibility, and it is a shared responsibility with the Under Secretary for Acquisition and Sustainment, to ensure that this program is sufficiently overseen and that we are doing this soundly and in line with the requirements as they have been laid out.

Senator CORNYN. So the Department of Defense is responsible?

Secretary HARRIS. The Department of Defense is responsible. And we are fully committed to making sure that this is the path to success for NBIS as we move forward.

Senator CORNYN. Well, it is no surprise to me that a program as complex as this that is overdue and over budget when apparently the most basic requirements were never identified initially; is that correct?

Secretary HARRIS. I think the requirements were outlined in Trusted Workforce 2.0. I think what we had was a breakdown in how those requirements were being managed into technical requirements for the development and how we were taking account of the delays in that process. And that is something that we are seeking to remedy immediately with more proactive oversight from the Under Secretary of INS's office in partnership with DCSA as we look to make sure we put this on a sound foundation.

Senator CORNYN. My time is overdue.

Chairman WARNER. One, I think you can all get nod. Dixon on classification. The other folks who are here, it's more on security clearance reform. But to add kind of insult to injury, you know, you got a thousand people at DCSA working on this, and a thousand

people at Peraton, the contractor, working on this and why nobody raised their hand earlier is something we're going to get to at some point today.

Senator CORNYN. Well, Mr. Chairman, if I could just add? The fact that there's a couple thousand people working on it doesn't mean that they know what they're doing or they're working in alignment toward an achievable objective on a timely basis. To me, that seems like the biggest problem here is lack of leadership and a lack of any accountability. And I grant that they're working on it, but I don't think that's a great answer.

Chairman WARNER. We do have new people in because it was—I wish we would have done this when the prior people were here so we could, you know, appropriately scour. And again, when we get around to another round, Dr. Plumb has got—because she's got a team that has been helping try to help figure this out as well.

Senator Bennet.

Senator BENNET. Thanks, Mr. Chairman, and I appreciate your mentioning that.

Dr. Plumb, that's actually where I'm headed, so I appreciate it.

Mr. Chairman, we have heard what a disaster the development of the National Background Investigation Services has been. And it sounds like, I hope, the review team has a clear understanding of what needs to happen to get this back on track. And I look forward to regular updates on the progress.

Others have covered the costs here. I want to focus on the schedule delays.

GAO reported in June 2023 that 16 of the 25 major IT business programs at DOD reported cost or schedule changes since January 2021, including 12 that had cost increases ranging from $43,000 to $194 million; had scheduling delays. I think there were 12 ranging from 3 to 33 months. And program officials attributed the changes to factors such as new requirements and unanticipated technical complexities that I'm sure drove scope in some way that might have been predicted, I guess.

But my question is broader than NBIS. It gets at the pattern of large-scale IT acquisition and software development across the federal government. The Chairman mentioned FAFSA and our veterans' health systems, but we could list what feels like an endless, endless, endless list of examples. By the way, examples where people are here to do the work, but never here for the accountability when we're doing our oversight. The IRS, you know, comes to mind, in my mind, actually recently as a decent implementation. But I'll put that to one side.

Dr. Plumb, in your statement for the record, you laid out three key points that this team will adopt: fixing the data, architecture, and adopting a modern approach; building the right team with the right skills and technical acumen; and adopting digital transformation best practices.

My question is, why can't we seem to adopt these principles across the federal government or at least in the IC and the DOD? Until these principles are mandatory, we're going to experience these failures again and again, wasting time and money and failing to deliver for the taxpayers. Would you like to say a word about that, Dr. Plumb?

Dr. PLUMB. Thank you, Senator. I think maybe the way to start this is, fundamentally our acquisition models in the U.S. Government and the Department of Defense in particular have remained hardware-centric. So we fund them in similar ways to the way we fund hardware procurement. And we use future delivery as our milestone markers for progress on them.

Companies that manage IT successfully with minimal disruption to users have a more continuous integration and continuous delivery and deployment pipeline process that. for instance, only takes software offline for very short periods of time to do upgrades and invests 70 to 80 percent of the total program costs into the backend data architecture and infrastructure as compared to the frontend user interfaces and features.

So inside the broader question of software acquisition, while we have authorities and the software acquisition pathway, the traditional program management oversight and processes have tended to drive focus on the wrong areas. That creates both a prioritization problem where prioritization is on frontend user interfaces and new features rather than backend investments and funding issues because those backend technical complexities cost money and take extra time.

In the context of NBIS, driving our recommendations is really focusing on those backend improvements, keeping what we can, building new things where we need to and then marrying that up with an agile continuous process for software development and delivery so that we don't face these problems again in the future.

And I'll just close by saying that while we, of course, want to get to the point where we're meeting the full set of the requirements, there's no point at which this is "done." And I think moving to a mindset where this is a continuous development and improvement process, that we'll continually manage and upgrade the backend technology and frontend features, is part of what can prevent this in the future.

Senator BENNET. Dr. Plumb, with the last 30 seconds that I have, could you talk a little bit about the Defense Digital Service? Is this the type of team that we can bring in that agency, working with either the principles that you've described or some rationale, at least, could help make a difference in these kinds of implementations?

Dr. PLUMB. Absolutely. The Defense Digital Service focuses on—they serve as our chief product office inside the Chief Digital and AI Office in the Pentagon. They focus on what we call product management approach to delivery, which means they combine a product manager who owns a roadmap in that Agile development process oversight with software engineers and user experience designers and researchers.

The idea of what we call product trio is to focus on turning the requirements that come in from customers into technical requirements and roadmaps and then ensuring that there is a systematic execution of those that are linked to continuous testing and user experience. And this team is one that we apply to major issues and concerns inside the department that rise to a priority senior-leader level like NBIS.

Senator BENNET. Thank you, Dr. Plumb, for your oversight of this. It's going to be hard to get to the bottom of all of it and I'm grateful that you're making it a priority.

Chairman WARNER. Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman. Away we go.

I think I really want to focus on one particular issue to begin with. And I think, Deputy Dixon, I think I'm going to focus with you simply because you come with DNI. What I'm curious about is we're doing our best here to identify and to be able to get folks in for security clearances and getting them through is extremely frustrating and it is in all branches of government. But at the same time, we want to make sure that we keep these individuals and that they feel that they are appreciated and that their service is meaningful and that basically we have their back.

The reason why I lay it out that way is because most recently, for the second time now on a "60 Minutes" display, we talked about the AHI or the anomalous health incidences in which individual members who are well respected within your community have clearly identified health issues that they attribute to specific identifiable incidences that have occurred.

Now we've had classified briefings on the topic and I understand that this is a very sensitive area. But I think for the individuals that are outside of those meetings that we have, individuals that are within the community, I think we should publicly talk about how we are going to address their concerns. And probably to the American people that this is not something which is being ignored or put on the back shelf.

Can you share with us, first of all, within your office, who is responsible and accountable for actually chasing down what is going on and not just simply the fact that we know that these incidences are occurring. There's a recognition of that and we respect these individuals. But there doesn't seem to be an attribution or a discussion of the attribution which has occurred. Could you perhaps in this open discussion at least give us some assurances that this is an ongoing thing that is going to get followed up on?

Director DIXON. Thank you, Senator Rounds. And absolutely, we are. Our first priority is taking care of the individuals within our community. So, our employees, their family members, whoever is experiencing health challenges as a result of whatever the cause of the thing is. We have from the top levels of every agency made sure that it's very clear that whatever they are experiencing should be reported. And once reported, we should do our best to get them the kind of help that they need. If that ends up being a payment out of the Havana Act, that is one route that they can go. But making sure that they get them quick medical care.

With respect to the side of who's actually looking for and who's going after it, it's really an entire agency—it's all of IC process, so it's not just our organization.

Senator ROUNDS. If it is, with all due respect, if it is everybody, it is nobody. Somebody's got to be in charge. I guess that's what I'm asking is, who is in charge of this very serious issue?

Director DIXON. It has to be, because the information that we need to collect is collected by different agencies, different agencies are responsible for different parts of it. The DNI has very clearly

stated that it is our plan to not only take care of employees but to try to close those intelligence gaps that have kept us from being able to do the attribution that you're talking about. So the DNI at the top, ODNI can be in charge.

Senator ROUNDS. Okay, so——

Director DIXON. But we alone can't do it.

Senator ROUNDS. Within the ODNI, the Office of the Director of National Intelligence, somebody has to be the person responsible for accumulating, acquiring, and pushing for this information. I don't need that name here, but is there a person who is responsible for getting this done?

Director DIXON. There are different people responsible for different parts. The part of collecting the reports from across the Community, yes, there are individuals who do that. The part of making sure that the agencies are out collecting information so we can close those intelligence gaps, yes, we're overseeing that as well, so there is not one person doing both parts; but because one is focused on the work, the people, and the other one is focused on the adversary or whatever may be causing these things. So there are individuals——

Senator ROUNDS. And how about the technical side of this? Is there a person working on the technical side of who is using what type of a weapons system or a technology? Do we have another person responsible for chasing that down as well?

Director DIXON. The folks that are overseeing the collection side are also working with those who have the technical capabilities.

Senator ROUNDS. So now we're down to just two people basically that are working on this or that are accountable for putting this all together?

And is somebody overseeing those two individuals or is that directly reporting to ODNI?

Director DIXON. Within ODNI we have individuals overseeing them. So those that are overseeing what's happening in the Community with respect to collection as well as what's overseeing that the guidance that we're putting forth on how to take care of our workforce is being followed, yes, correct.

Senator ROUNDS. So we have one person in charge of each of those two? At some point somebody's got to be in charge.

Director DIXON. I think if you were to ask my boss, Director Haines, she would say she's in charge. She is the place where it ends. And so, by default, I am in charge as well. We will make sure that our communities are doing what we have provided guidance for them to do, which is to take care of the people and to do our best to close the intelligence gaps.

Senator ROUNDS. And I don't mean to belabor this, and I'm already over my time, but it just seems to me that unless there isn't somebody who can look at us and tell us, this is my responsibility. I'm in charge of getting through this thing. I'm responsible for having this thing fixed. Then it means that it's going to be on the back side and it's going to get delayed and we're not going to get it completed in a timely fashion.

I simply bring it to your attention because I think we're going to have to continue to ask that question until we get a direct answer about somebody who is responsible for following this through

just to make sure that those folks out there that are suffering through this and that may be impacted by this in the future know that it is not on the back shelf.

Director DIXON. Okay. Okay.

Senator ROUNDS. Thank you, Mr. Chairman.

Chairman WARNER. I would say, Senator Rounds, I think, you know, the vast majority of folks affected were CIA. And CIA was taking the point. But there were then people that were affected, DOD, that was kind of a separate chain. And then there were some Treasury. So you know, it was across a series of departments.

Senator ROUNDS. Oh, no question. But the problem is, unless we've got somebody responsible for actually chasing this stuff down and everybody's looking at each other, we're not going to get this thing fixed. And it seems to me that we owe it to the Intelligence Community, to the folks that are actually doing the hard work outside of our boundaries that we're going to follow this thing through.

And that we have not simply said, we know something happened. We don't know what it is and we're not going to do. And until it comes to us, we're not going to chase it down.

Chairman WARNER. Well, we have a hearing I think on July 31st on this topic exactly. And you know, again, I think we need to get it fully aired out.

Senator ROUNDS. Excellent. And hopefully by then, we'll know who the folks are that are actually chasing it down. And they can share with us what they've gotten done. Thank you, Mr. Chairman.

Chairman WARNER. Senator Kelly.

Senator KELLY. Ms. Harris, when was the initial RFP for the NBIS program? When did we start?

Secretary HARRIS. So I will refer to DCSA for the specifics on the contracts, but this has been a multiyear process that——

Senator KELLY. Well, when was the contract awarded?

Secretary HARRIS. Okay, I will defer to David for the specifics on that.

Senator KELLY. The first one with Peraton.

Director CATTLER. Senator, this program was begun in 2016 as a DISA effort, so the first RFP would have been issued then.

Senator KELLY. You know, a typical software program—you come up with a set of requirements, you come up with a plan on how you're going to develop the software, how you're going to verify it, how you're going to test it, how you're going to make sure all the parts work together, make sure it's integrated with other systems.

Pretty early in a program you fix requirements. And then, you say this is it and, contractor, you need to build this.

Software acquisition often goes—one of the ways it can go kind of sideways on you is if you keep changing the requirements. I heard, and I can't remember who said it, maybe Dr. Plumb, that you now have a new requirements management process that you're putting into place. So, it sounds like the requirements are still being developed for this system that we started to acquire in 2016.

That could be the problem. I mean, I have yet to hear what the real problem was that caused this to be delayed from something that started in 2016, that was supposed to be delivered in 2019, and now we're in 2024, and it sounds like we're still working on requirements.

Let me ask one question. The other possibility or maybe it's a combination of a few things—I think somebody mentioned production challenges and difficulties and requirements was thrown out there—is the contractor. You know, software is—it's hard. I'd say it's difficult. It's different than manufacturing hardware, obviously. It presents its own set of challenges.

So are you having problems with the contractor being able to write the code and then verify the code and test the code or is it the thing I started with, which is you keep changing the requirements and they can never catch up?

Secretary HARRIS. So I'll start with the requirements and then I'll defer to David on the specifics on the engineering. I think when you hear us talk about the requirements process, what we have is, for something like this, we're getting real-time user feedback. The federal customers are using it. There are things that will need to be integrated into future development cycles. Right now, what we did not have was a rigorous way for us to take those requirements and kind of look at them against a technical roadmap and understand where they would affect the development timelines.

And so that is a place where the Under Secretary of INS's office will be taking an active role to make sure we have a better set of processes to make sure that as we're getting feedback from users as they're using NBIS as the capabilities roll out, and there are requests for new and different things, we understand the effect they may have on our long-term development timelines.

Senator KELLY. Was that built into the contract? That you were going to continue to feed back new requirements to them as this was tested and they would have to make changes?

Secretary HARRIS. So, I think as we are onboarding folks into this process, right, there is an expectation that as we are developing, under Agile methodologies, that we would be getting user feedback, and we would be ingesting that into future deliveries. I think what we did not have was a really mature infrastructure to translate government requirements into technical requirements, as Dr. Plumb mentioned. And so that's a key finding from these 90 days is we need to get more rigorous around that.

The overall requirement is Trusted Workforce 2.0. The requirements for what NBIS needs to deliver that end-to-end IT system for vetting have been clear from the beginning. The enforcement and the kind of interaction of that with the technical development and the user feedback is where I think the rigor needs to come in. I'll defer to David for specifics on the contractor performance.

Director CATTLER. Senator, we started with a firmly-defined set of requirements. We had requirements first from the Secretary of Defense in 2016, as the Acting Under Secretary has laid out about that end-to-end system. Those were complemented by further requirements when the Administration's agenda in that timeframe of 2018 for Trusted Workforce came together. Those requirements though are essentially the same, they're just at a higher level when you combine the departmental requirements and cross-governmental requirements.

I'm going to give you a perspective from inside DCSA now looking at this. What I would say is that they were realistic, the requirements. They were achievable. But my agency did not have a

firm understanding of the complexity of the technical features nor how exactly to approach those and accomplish them.

Now as Dr. Plumb has also said, it would seem from our review, from my review now as the Director about 100 days, that we did in fact, as Dr. Plumb said, focus first on features and a bit less on functional capability delivery.

And there's a related point here then about cost, about legacy system sunsetting because if, for example, we had taken an approach to prioritize the sunsetting of the legacy systems and especially those that cost the most first, we could have wound up in a different financial picture at this point, if not actually had delivered more capability at an earlier time.

Senator KELLY. Was the contractor aware of the complexity of the system? Do you think they were pretty honest with you about the challenges that they were going to face?

Director CATTLER. Senator, I think there's a couple of things in there. I'd say one is, yes, I think the contractor has been honest with the government about what they can deliver, and they've done the work as the government specified it. But at the same time, the government reserved for itself the role of being the software integrator. So in that, we asked for certain things that's—Senator, that's why I'm emphasizing the significance of my agency's decision making about interpreting their requirements.

Senator KELLY. Have those individuals within the government that were going to do the software integration, have they done software integration on any programs before?

Director CATTLER. Yes, sir. My new NBIS program manager has deep and lengthy experience doing this for the Army for enterprise information systems. It's one of the primary reasons why I selected him to be the program manager.

Senator KELLY. Could you give us an example of Peraton, what else they have built?

Director CATTLER. Sir, in this case, all I could say now is that what I rely on Peraton for are these software services related to NBIS and also for a very extensive effort related to field operations for background investigations themselves.

Senator KELLY. Well, thank you. Thank you, Mr. Chairman.

Chairman WARNER. Let me make a try at this. This is my kind of understanding. And I welcome anyone on the panel to correct.

This is a hard issue. We've been trying it for a long time. Conceptually, I think the Trusted Workforce 2.0 is a great goal to get to. DCSA is a relatively new entity. And they think they got the big picture requirements in place. But candidly, from conversations I've had with predecessors and others, DCSA did not have the technology knowledge of how complicated these requirements would be to actually build and build at scale. One of the key things that Mr. Cattler just said was my new NBIS supervisor has got this experience, which previously they didn't have that experience.

And there was a while—and some of the predecessors who had positions here were either—they couldn't, wouldn't, or shouldn't kind of say "this is above my knowledge level." So you have the problem that the requirements—and look at the—we all see the placemat here. We've all read and seen the gazillions of these. But we're taking a system that was really antiquated and trying to

come up with this new cutting-edge idea. It's a good idea, but boy, the implementation has been really bad. To compound this—and Peraton does a lot of work in other parts of the IC—You know, I think we had a fixed-price contract. That's why we came up with this notion "well, it's going to be $700 million bucks." And I worry that there was not even any incentive because I think at some point along the way, even though they may have been—I don't think DCSA got the requirements right specifically to the technical capability that they need to draw but probably the contractor bid against an inappropriate set of requirements. But what makes me crazed a little bit is that somewhere along the way, I think even if they had built to the requirements that they had opted for, they couldn't scale those anyway. And because—I wonder—and again I'm anxious to be contradicted on this—is you had folks at the contract saying, "well, we have a fixed price contract. As long as we hit these things, we're going to be fine" even though I think probably people had to have known, oh my gosh, what we're building can never scale to the needs of the whole classified and secret workforce.

And maybe DCSA, you didn't have enough folks or maybe we were so far along, they kept with a hope and a prayer that this would figure itself out And we had a holy heck moment. And we were pushing. We were told things were going along. And frankly, only because of an inadvertent loss of 9 terabytes of data that they did recover that we even found out about this. I mean, when would we have known?

I mean, at some point, the game was up, because there was not going to be any plan where they would have had a fully operational system by September of '24, even a year ago. And then there was like, as the deeper we got into the rabbit hole, it was more like holy heck, this is not a short term, this is a massive screw up.

So we got 850 million bucks that we've spent so far. We got $850 million of maintaining legacy systems that we wouldn't have had to spend if we would have gotten the new systems in place by 2019. I think Secretary Harris and Director Cattler are working their tail off to try to get us this output of what it's going to take in 18 months and how much it's going to cost. But thank goodness—and I hope this is where we've got to figure out your capabilities overall—what Dr. Plumb's group is supposed to be doing is they're supposed to be, as Senator Bennet said, the Technical SWAT Team to come in. Because I don't think you had the Technical SWAT Team at DCSA. And how we get at the contractual obligation that if the contractor has got the technical knowledge, why don't they raise their hand and say, hey, we're building your stuff, but by the way, we're not building you something that can scale.

We got to figure out how we think about contracting. And one thing I would also say is if there are other—the Committee wants to work with you. If there are other legislative authorities you need in this software management, we're willing to take a good hard look at that.

But is the characterization of how we got here that I just laid out, am I right? Am I partially right? Am I wrong? Who wants to take that on? Look, lots of hands going, but so—please?

Secretary HARRIS. So I think at the beginning we expected we would gain co-efficiencies by putting this at DCSA between mission and what mission—what this is supposed to deliver. I think what we have realized is that a program of this scale and complexity, to exactly your point, needs a whole-of-department approach.

So I think that's what you're seeing reflected here today. We need Director Cattler's leadership. We need Dr. Plumb's squad. We need Under Secretary LaPlante's acquisition oversight. We need our CIO looking at this against other software systems in the Department. And we need Intelligence and Security to make sure this meets the mission. And that is what we needed.

And so I think the road you laid out, Senator, is exactly right. But I think what you need is the team you have right now looking at this with the——

Chairman WARNER. It wasn't that the fact that—but if we had been smarter in 2017, 2018, shouldn't we have known that we were asking this relatively small entity to take on a task that was too big for its britches? And there are capabilities inside of DOD that can [audio disruption] there are capabilities.

And that's what I think Secretary Harris is saying is we're going to try to bring all the capabilities of DOD to the table. We should have probably had that. We probably were expecting too much from an agency that was not fully prepared to execute on this.

Senator KELLY. Can we get back to the contract, though? So what happens now? I mean, at one point, the contractor, the prime contractor, sent an invoice for something that was beyond $700 million, right? And they had to explain themselves. I mean, what was their explanation? And then have we resolved that issue or is the cost going to just continue to grow? Because I imagine my guess is because, you know, I've seen this before, the contractor says, well, you're changing the requirements on me. We had a fixed-price contract to build this box that does these things. And now a few years later, you've got—we've deployed parts of this and you have the end user is saying that they want changes.

And you're feeding these changes back to the contract. And they say, well, we weren't contracted to do that. So then they say, well it's going to cost you this much more. And every change order is going to be, you know, whatever—$10,000 for every single change.

Has that portion of this been resolved?

Director CATTLER. Well, yes, sir. And that's why I've said my second basket of issues. We looked at in this 90-day review was in fact procurement. And that's, you know, as I said in my statement for the record, that's everything from not just how we got here, but also to how we need to move forward. Do we have the right contract vehicles? Are we incentivizing and disincentivizing properly to hold a contractor accountable? Is the government clear in terms of what it's calling for? Do we have the right expertise? As I say, we didn't just need technical expertise on the IT. We also needed to take a hard look at the procurement.

I mean to link both of your interventions. What I would say is I also agree that it would seem to me it was a lot to put on a new agency to tackle this, as well, as the agency was standing up. However, there was too much authority vested in the previous incumbent in my role, in this context. And that's why I wholeheartedly

agree with the elevation of product ownership, the program ownership up to the Under Secretary for Intel and Security and the acquisition decision milestone authority also being elevated away from me at DCSA to the Under Secretary for Acquisition and Sustainment.

Because in effect, my agency was allowed to call the shots on how to interpret the requirements, figure out what the procurement approach should be, figure out what the technical details then were inherent in all that development, take the decisions about contractor performance and compliance, what information was reported out for oversight.

So if I may, Senator, get back to both of you, because you've also asked, is there anything that needs—just to clarify a couple points that I think are important. The first is that you've asked the question of when we would have—when you would have been notified and when you would have found out. And I think two things I would say here, just so at least, as the DCSA director, I'm clear on what I communicate to you.

The previous Under Secretary for Intelligence and Security came before this Committee in November of 2023 and did inform you that largely the program was on track. My agency did not inform the Under Secretary for Intelligence and Security and the office that we were substantially off track and would not meet the 2024 deliverable until after that hearing had concluded.

So I think that's one point I just want to make sure that I share with you. And the other thing I would say is——

Chairman WARNER. Which is a big freaking deal.

Director CATTLER. What's that?

Chairman WARNER. It's a big deal that he wants——

Director CATTLER. It's a big deal, yes, Senator, that's why I'm making sure that I clarify that.

The other thing I would say is that on your observation about the OPIS outage, so this is one of the OPM legacy systems that we rely on essentially as a data storage system for the records. I do not think that the two things, NBIS and OPIS, are actually not linked in a direct causal way, meaning that the OPIS outage that occurred would not in itself have triggered my predecessor nor anyone else to come here and say that NBIS would not be delivered on time.

Chairman WARNER. But I believe what happened—and you weren't there—but I believe what happened, and some of the folks who were working on this are not here now, they're over with Dr. Dixon, but was that we—people came in and informed well, we got this problem. We're going to get it fixed. We've lost 90 terabytes of data, but we got a backup, so we're going to find it. And oh, by the way, there was not a linkage that that loss was related to NBIS. Oh, but when in that notification around the 90 terabytes, oops, that was when we were notified by them.

So I don't want to imply that they were linked, but it was like simultaneous notification.

Director CATTLER. They're coincident in time, Senator. My review of this—and again I had my Inspector General helping me with this also. But my review of this is—is we did conclude the investigation into the OPIS outage about my first week in the role here

as the director. We already knew internally that we had a real problem on our hands here. We'd known for quite some time about NBIS, but it didn't become clear enough to actually, I think, pop a flare and go back to Intel and Security and say, clearly, we're not going to meet that milestone.

So, all I'm saying is, Senator, both of these problems were quite bad for what they—one, OPIS for what it could have been, because as you've said, we did recover the 90 terabytes of data, thankfully. That was a failure to follow internal controls, meaning that we had an employee, some employees together, that did not follow the proper procedures for the ways in which we would clear storage memory on the system. And instead, issued an order that wiped out 90 terabytes of data.

Now again, it's great, we have magnetic tapes that have the backup on it. But the root cause of that is a failure of accountability, a failure to follow proper procedure. Concurrently, we had longstanding problems related to NBIS.

Chairman WARNER. This is where I think Senator Kelly and I were both trying to hit a little bit on. I was informed or told that—going back to the fixed-price contract, the nature of the contract, there was no incentive for the contractor to say, oh, by the way, we believe we are contractually meeting your requirement. But by the way, we could never scale this to meet the full needs of the Community.

Director CATTLER. Senator, I'd say——

Chairman WARNER. Is that fair, or not fair?

Director CATTLER. I'm not sure it's entirely fair, but it's not unfair. I think what I would say in response is, the contractor doesn't get paid unless the software they develop meets the specification and is successful. So, in that regard, the government gets what it pays for. The government gets what it tells the contractor it needs to do.

However, it is not the contractor's primary responsibility to inform the government that it might not scale or it might not be able to be aggregated as the government performs the role of the software integrator.

But you could ask the question of whether it's incumbent upon the contractor to inform the government: Hey, government, your ideas don't make sense.

Chairman WARNER. Right. Well, that wouldn't—you know, especially if DCSA didn't write the specs. But isn't there some obligation, moral or otherwise—maybe not legal—but moral or otherwise to say, hey, we're building a machine that's not going to be able to service the scope of the problem that we're trying to address?

Director CATTLER. Well, Senator, I can't comment too much on that piece of it in the past, but just to say that again, as we review the procurement approach and the ways in which we will move forward, these are all key factors we have in mind.

Chairman WARNER. And the company's got a good reputation. Let me state that. The company has—the contractor's got a good reputation. I remember as a new Senator having a lot of contractors based in Virginia, in the beginning of the Obama Administration, I thought I'm going to figure out defense contracting.

And the then-number-two at DOD came over and brought in four contracting officers and twelve volumes. And I was cured of my thought that I was going to fix this in any shape or form. But at least, in terms of what we've got—ability to, say, have purview over, and this is one of those areas where we're going to stay obsessed about this until at least as long as I'm here.

Is there legislative authority? And maybe this is for not just for Secretary Harris and Director Cattler, but Dr. Plumb or Dr. Dixon, either in terms of a stick of a penalty if you don't inform or an incentive if you do—oh, by the way, we'll give you a little extra spliff here if you tell us, government, that we are completely screwed up in our requirements, or we're not building something that's going to meet the problem.

Director CATTLER. Senator, that's just not the way we built that contract architecture. That's not to say we couldn't in the future or that we shouldn't, but we did not.

Chairman WARNER. Right, but again, this is not just your problem, it is across—as we all cite our various examples. But it is a little frustrating that when we see—and it's not like every large corporate software problem project doesn't have problems. But we do seem to have an extraordinarily higher failure rate on big software projects in government than almost anything else.

And Dr. Plumb, it looked like you were going to hit your button.

Dr. PLUMB. I was just going to add, Senator, I think a big part of the issue that our Defense Digital Service team identified, that we're working closely with DCSA, is making sure the right technical talent exists inside the government to vet and review what's going on. In this case, just as an example, the decision was made on this contract in 2018 to have essentially a low code solution, which means it's like a sort of simple drag-and-drop coding solution to solve a massive data architecture engineering problem, including with some legacy systems that use code that doesn't exist anymore, that people don't use anymore.

That's not traditionally—we would not consider that a best practice. We wouldn't even consider that an advisable practice because you want a true programing language, a Java or a SQL, to be able to manage the interaction between those databases in a flexible and continuous development way. So as just a concrete example, the lack of technical expertise in the government to review those types of decisions, the decisions to how to meet the requirements, which as were mentioned, I think were clear how to translate that into a technical solution was missing.

I think what we have now is a team of technical experts with our Defense Digital Services that are working hand in glove with the program management office and are working with that office to identify and hire inherent technical talent that will help DOD out.

Chairman WARNER. But let's take it out of DCSA. Let's take another part of the government, another part of DOD. You know, are we going to bring your SWAT team in on the frontend before we put these contracts out in other areas?

Dr. PLUMB. Well, that's what we're trying. I mean, yes, we're trying to do that for future solutions. I think better to solve it on the frontend of the procurement than the backend. And I think there

are broader efforts to do this across the department that don't that have technical talent in them that don't need us——

Chairman WARNER. But what you guys are doing in your Defense Digital Services, how long has that enterprise been around?

Dr. PLUMB. I think—I can get the exact answer, but I think since roughly about 2017 or 2018.

Chairman WARNER. Okay, so it has been around. So I keep thinking about, like, under the Obama Administration there was 18(F) and there were the digital services.

Dr. PLUMB. Right, exactly.

Chairman WARNER. It feels like these kind of crack SWAT teams, though, come and go inside the government enterprise in a way that we don't build that at least review part of the process in enough of our systems. Is that fair?

Dr. PLUMB. That probably is fair, I think. Inside of the Department of Defense, we've tried to establish this chief digital and AI office, my office, as the lead staff assistant inside the Department to oversee that data, data architecture, data oversight, data principles to help drive alignment both in how we build—the technical requirements we're talking—about and what the procurement requirements are. So what does it mean to be interoperable? What does it mean for the government to have data rights, so that that's baked into the contracts, the government rights, instead of trying to solve that problem over and over again? And that's work we have ongoing. And we have sort of large-scale initiatives underway to do that.

Chairman WARNER. And Dr. Cattler, you mentioned the fact that maybe your predecessors weren't aware or asked for too much power and authority without enough oversight. Or didn't recognize they didn't have the technology components. Is there a way to build in somebody with—you know, you got an agency with 5400 people. Somebody's got to have been willing to say, hey, you know, we're biting off more than we can chew.

Or are there any things—again, with your agency and specifically——. But are there other ways to build in some kind of incentive within the agency to say before we bite this, we ought to think twice or——?

Director CATTLER. Well, yes, Sir. And I think that these are some of the issues I'm alluding to when I talk about having a culture of accountability. We also needed to look hard inside ourselves as well and determine, were we organized in the proper way, broadly, but specifically on these issues, to be the right people in the right places, and have we segregated the decision authority in a way that will give us, first, internal checks and balances and also some different expertise and some differences of view as we take these decisions.

So, I already mentioned we lacked a firm understanding of the complexity, the technical features required to deliver. We underestimated the timelines it would take. Now, those are both about expertise. We had a shortage of critical technical/agile acquisition and integration skills within the program when the program was transferred to us, but then also over time within DCSA.

When I talk about leadership, I think it's important to point out I also hired another new program executive officer. The role of the

program executive officer here is to look across in my agency, nine programs—NBIS is but one of them—to make sure that they're compliant with proper acquisition strategies and the documentation is robust, is also compliant.

Chairman WARNER. Well, why were we able to set up DCSA without having a program executive in place as part of the initial structure of the agency?

Director CATTLER. Well, Senator, in this case, we had the two billets. But for a period of time, the NBIS program manager and the program executive officer were in fact the same individual person, which is why I'm saying the decision authority was a bit too concentrated.

Chairman WARNER. It's been a while since I've been in business, but I realized you're supposed to have these functions check each other or somebody overseeing the actual program management itself at somewhat of a checkpoint level.

Director CATTLER. Senator, I completely agree. And again, if I'm not in a position to record properly diagnostic and accurate internal information, nor report it up to my higher headquarters where I'm held accountable, then it's easy to see where you'll have a breakdown in process that can, over time, lead to these sorts of problems that we're experiencing with NBIS. And that's why, again, I say this 90-day period that the Acting Under Secretary called for this 90-day review has been critical and really fruitful, well timed, because she did bring in new leadership at the agency level. By extension, then, brought in a new PEO and a new program manager. We're able to look comprehensively with partners from CDAO, DDS. Counted on GAO here also to go back through those reports. We invited them in. They came in to see me at my invitation the first week of May. It was just critically important that we brought the right people to the table.

Chairman WARNER. Well, I would ask again: if there are additional legislative authorities, but I do think you know, and maybe we are not being harsh enough. I mean, it's a strange time in lots of government at this point. But you know, to me, in many ways, this is in a different setting with maybe a different membership here that was more willing to just kind of flog the heck out of you guys.

This is as, as you know a holy heck—government abuse contract problem as pretty much anything I've seen. You know, you could make a lot of hay with how this started, a new agency, we're five years behind, we didn't get fully notified, you know, hey didn't——. Your predecessor, Secretary Harris, wasn't even fully notified in an appropriate way. And where what was supposed to be probably wrong-sized at $700 million to start, but we're roughly $1.7 billion now, five years late with another 18 months and no cost estimate to go. I'm glad we got the new team here, because if it was the old team, it would just be too easy not to just whack the heck out of you guys.

But the next time you come, if we're not seeing marked improvement—and you just need to be straight with us, if it's——. I do think this is broader than your respective roles. But the incentives to get the contractor to raise their hand, that says, hey, we're not building something that can scale or we're not building something

that's going to really meet the need or within the agency. There's got to be somebody that kind of felt this doesn't pass the smell test. And I obviously think—remember when your predecessor came in and said, we're going to bring it up into Big DOD and bring more of the expertise. How we let it get this far along the way is a real challenge. Because if we go back to where we start—and Dr. Dixon, you're not going to get away completely unscathed here—where was the PAC through all of this?

Director DIXON. Uh, Senator Warner, thank you for that. You're absolutely right. We did not recognize that there was an issue. We talked about NBIS every time we met as PAC principals which was very frequent. But we were also working across all the other things that we're trying to deliver as part of Trusted Workforce 2.0, so we did not dedicate enough time diving in and asking the hard questions.

I think we all made assumptions that some of these other levels of oversight actually existed when it turns out that they did not. But we did not ask the questions that would have gotten us to realize that there was a problem earlier.

Chairman WARNER. But again, that doesn't totally pass the smell test either, because we knew this was a problem. It was supposed to be delivered in 2019. Didn't somebody say in 2022 or 2023? Then again, you could argue if we've asked that question, too, but you had a more direct ongoing responsibility. Why didn't somebody in the PAC say we ought to dig into this a little more?

Director DIXON. I think when the group of us that—the former people that were at the table with me back in March of '23, all of us came in '21—and so we actually thought that we were on track for the redo in the new process, in the new plan for NBIS. And every time we looked at the slides, there were not so many tremendous changes in the deliverables to raise the concern to us. It looked like they were minimal slips that happened.

Chairman WARNER. So, when you came in, in '21, they were still expecting a September of '24 deliverable?

Director DIXON. Correct. Correct. I don't remember the exact date, but it was definitely something in the future, beyond '21.

Chairman WARNER. But did you have in September when you came in, in '21, did you have a plan that says: Okay, by September of '24, we're going to get it done and it's going to cost x——? You must have had some presumption of what the costs were going to be.

Director DIXON. I'm absolutely sure that we did. As PAC principles, we sort of were all looking at our own particular pieces of the puzzle. And so, I don't know that we were——

Chairman WARNER. Well, how do we make sure the PAC doesn't miss this again? Or, because, again, NBIS is just one piece of this glorified idea. I mean, I had a lot of problems with the previous Administration, but the previous Administration did at least start to take on this and help work to bring down the backlog.

But I feel like we knock out one of these issues—we knocked out the backlog. Then we had to deal with the adjudication piece. And you know, again, I'm preaching to the choir here when we, you know, didn't have enough polygraph trainers. Then we didn't have people to train the polygraphers.

You know, I think we keep knocking these things down, but then you get this. We got this glorified great new system and this is an embarrassment.

Director DIXON. I agree. What I can say is, I am much more comfortable now with the level of oversight that's going to be provided with Dr. Plumb. With an acquisition and sustainment as well as with what the Honorable Harris and her staff are going to do. This is what should have been in place beforehand.

Now that it is in place, we will do our part.

Chairman WARNER. Well, one of the things we can ask the PAC is how many other of these potential ticking time bombs or not-ticking time bombs, potential, oh, my gosh, we're not going to hit these metrics?

Director DIXON. Very little of what is left to be delivered is IT solutions. Most of what's left to be delivered include how do you take the guidelines and the standards we've created and then roll them out into the workforce. How do you get everyone ready to do the types of investigations? And so a lot of things are dependent on NBIS. But NBIS is by far the largest IT part of Trusted Workforce 2.0.

Chairman WARNER. Oh, well, I would say this. I have great respect for you. I also have great respect for your predecessor, Sue Gordon.

She promised me she was not going to leave the job until we had reciprocity with CIA.

Director DIXON. We are making a great deal of progress on reciprocity.

Chairman WARNER. Across the whole Intelligence Community?

Director DIXON. Across the Intelligence Community. When you talk about specifically someone that's going from a similar level of security classification, or security clearance needed, that person, as I mentioned before, that process can take as little as five days when it is apples to apples. In many cases though, it's not. You're going from an agency where the responsibilities you have in one job are actually less and require less sensitive information than the other one.

And so, then you have to look at, Okay, does the person need——? Do we have to go back and look at continuous vetting alerts? Did something come in between the time the person was hired in the one agency or the other one? Does this one agency, the second agency, now require medical screening or psychological screening or a different kind of polygraph?

So, there are other things that make it not a simple movement, but when it is exactly the same level of clearance, same responsibilities and same process from one agency to another, that process is very quick. And we are working on the other one.

Chairman WARNER. Okay. And is there any way as well that I can hold our former staff director, Mike Casey, responsible for anything screwing up going forward?

Director DIXON. Mike Casey and his organization are going to deliver a tool that's going to significantly help with reciprocity. And I'm absolutely sure that they are listening.

Chairman WARNER. On what timeline? Now he's—to your left.

Director DIXON. We are in the requirements-definition stage, and we may actually reach out to——

Chairman WARNER. Requirements definition stage, we may need Dr. Plumb's—or a team.

Director DIXON. Exactly. Exactly. I think we have some oversight that we're already talking about and how do we make sure that we——

Chairman WARNER. Honorable Casey does not want to be up here in front of this panel talking about this issue at some point in the future.

Secretary HARRIS. I am absolutely sure he would agree with that statement. [Laughter]

Chairman WARNER. Well, I'm disappointed that we're here. I do appreciate the new members of the team who are trying to get this, but we have to stay on it. You know, at end of the day, we get caught up on these details, but end of the day, we got to make sure we've got a security clearance process that works; that we can still recruit the best and the brightest into the Community; that our government contracting workforce cannot be delayed and you know, driven to not be as efficient because they have to waste so much time. And we didn't even get today to the whole question of smaller companies who don't even have billets based upon butts in the seats, so that your CFO, you make it the CEO is a clearance, but the CFO doesn't know.

And how do you have a CFO that didn't even know what the projects they're working on?

Director DIXON. We are actually making progress on that too. We heard you loud and clear that there are individuals who can't charge to a contract who need to have clearances.

Chairman WARNER. Dr. Dixon? Right, who need to have you—their senior executive team has to have those billets or have to have those numbers.

Director DIXON. We're trying to work with our contracting organizations to actually make sure that can happen.

Chairman WARNER. I know. But that, respectfully, and I know you've only been saying it for two-and-a-half years, but I've had other people sit in this seat now for the 7 or 8 years now, almost 10 years, that I've been talking about it and I just don't understand why it's taken so darn long and why some of this is so hard. And maybe that will be the function of our next hearing.

For those of you at DCSA and NBIS, we've got great expectations. But I strongly, strongly suggest that if you've got a need for different authorities, I'd like to hear them.

Dr. PLUMB, I know you say this is not the way we structure software in government contracting, but maybe we ought to take some experiments.

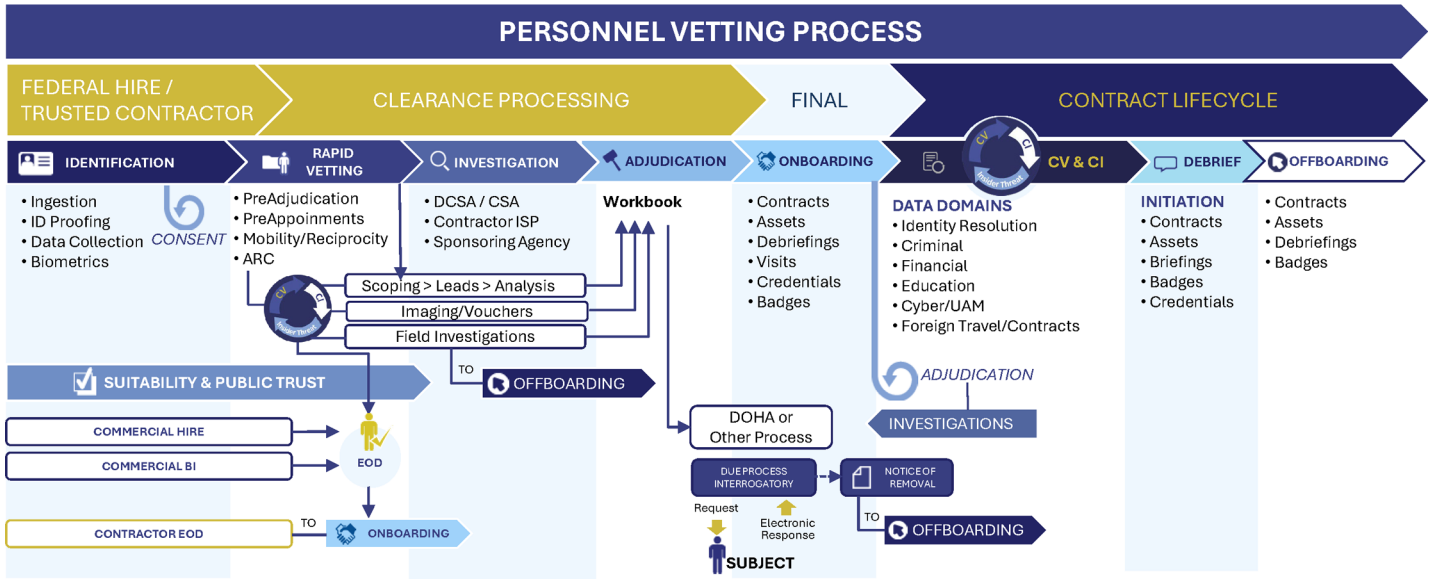
You know, we can call it AI. That means we can get funding for it no matter what if we call it AI in your office. But think about where we actually try to align the agency and the contractor's interest to come to the same technology-driven success goal which I think, again—and I don't think this is unique to NBIS but is too often a problem where they are not aligned.

I think I've driven all my other colleagues away. I was actually surprised that we got as many showing up as we did. But as long

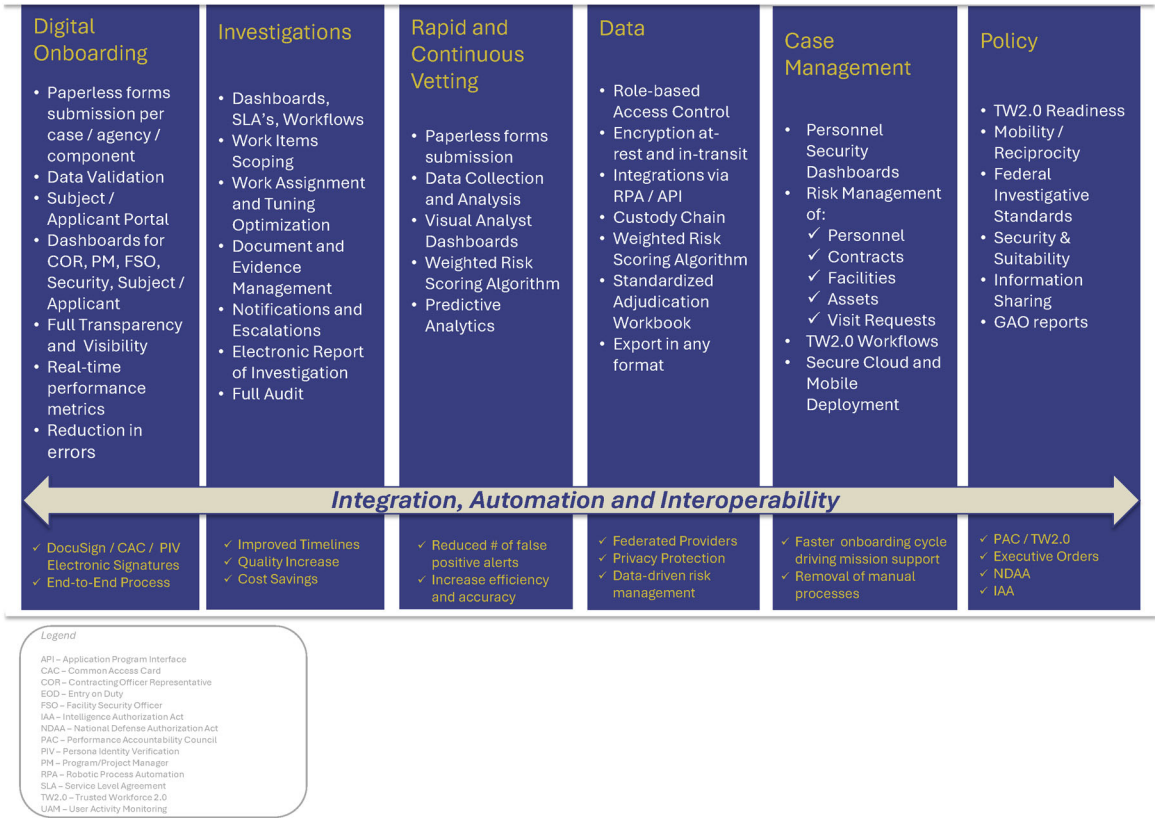
as I'm here, we're going to stay on this and we're going to get it fixed. We are adjourned.

Thank you.

(Whereupon at 4:40 p.m. the hearing was adjourned.)


PERSONNEL VETTING PROCESS
FEDERAL HIRE / TRUSTED CONTRACTOR
CLEARANCE PROCESSING
FINAL
CONTRACT LIFECYCLE
IDENTIFICATION
RAPID VETTING
INVESTIGATION
ADJUDICATION
ONBOARDING
CV & CI
DEBRIEF
OFFBOARDING
• Ingestion
• ID Proofing
• Data Collection
• Biometrics
CONSENT
• PreAdjudication
• PreAppoinments
• Mobility/Reciprocity
• ARC
• DCSA / CSA
• Contractor ISP
• Sponsoring Agency
Workbook
• Contracts
• Assets
• Debriefings
• Visits
• Credentials
• Badges
DATA DOMAINS
• Identity Resolution
• Criminal
• Financial
• Education
• Cyber/UAM
• Foreign Travel/Contracts
INITIATION
• Contracts
• Assets
• Briefings
• Badges
• Credentials
• Contracts
• Assets
• Debriefings
• Badges
Scoping > Leads > Analysis
Imaging/Vouchers
Field Investigations
TO
OFFBOARDING
SUITABILITY & PUBLIC TRUST
COMMERCIAL HIRE
COMMERCIAL BI
EOD
CONTRACTOR EOD
TO
ONBOARDING
ADJUDICATION
INVESTIGATIONS
DOHA or Other Process
DUE PROCESS INTERROGATORY
NOTICE OF REMOVAL
Request
Electronic Response
SUBJECT
TO
OFFBOARDING

Personnel Vetting Capability Needs



Legend

API – Application Program Interface
CAC – Common Access Card
COR – Contracting Officer Representative
EOD – Entry on Duty
FSO – Facility Security Officer
IAA – Intelligence Authorization Act
NDAA – National Defense Authorization Act
PAC – Performance Accountability Council
PIV – Persona Identity Verification
PM – Program/Project Manager
RPA – Robotic Process Automation
SLA – Service Level Agreement
TW2.0 – Trusted Workforce 2.0
UAM – User Activity Monitoring