

Senate Homeland Security and Governmental Affairs Committee Holds Hearing on Information Sharing in the Era of WikiLeaks

[LIST OF PANEL MEMBERS AND WITNESSES](#)

LIEBERMAN:

The hearing will come to order.

Good afternoon and thanks for your patience. We just were able to -- Senator Collins and I vote early. And I want to apologize in advance, I'm going to have to step out for about 15 minutes in about a half hour, but I shall return.

In just six months and a day we will mark the 10th anniversary of the attacks of 9/11, and we will honor the memory of the nearly 3,000 people who were murdered that day in America. Our mourning over their deaths has always been compounded by the knowledge that those attacks might have been prevented. Certainly, that was the implication of the 9/11 Commission Report, had our intelligence and law enforcement agencies shared the disparate facts they had gathered, enabling us to connect the dots.

To prevent this from happening again, Congress passed several laws intended to strengthen information sharing among critical federal agencies. Those acts included the Homeland Security Act, the Intelligence Reform and Terrorism Prevention Act, and the Patriot Act.

Since then, the Executive Branch I think has made significant improvements in its information sharing systems and there is no question that far more information is now available to partners in other agencies who have a legitimate need for it. All this intelligence is further brought together at key nodes such as the National Counterterrorism Center where it could be examined by intelligence specialist from a variety of agencies working together under one roof.

And as a result, we've seen a number of successes in recent domestic and military counter-terrorism operations that I think were thanks to that kind of information sharing. I'm going to cite some of those examples in a moment.

This Committee's recent report on the Fort Hood attack shows that information sharing within and across agencies is nonetheless still not all it should be. And that allowed in that a case a ticking time bomb, namely Major Nidal Hasan, now accused of killing 13 and wounding 32 others at Fort Hood, to radicalize right under the noses of the Department of Defense and the FBI.

So we need to continue improving our information sharing strategies. Now, I fear the WikiLeaks case has become a rallying cry for an overreaction for those who would take us back to the days before 9/11 when information was considered the property of the agency that developed it and was not to be shared.

The bulk of the information illegally taken and given to WikiLeaks would not have been available had they -- had that information not been on a shared system, so the critics of information sharing argue. But to me, this is putting an axe to a problem that requires a scalpel and misunderstands the importance, misunderstands what happened in the WikiLeaks case and I think misstates the solution to the problem.

We can and must prevent another WikiLeaks without also enabling federal agencies, in fact perhaps compelling federal agencies to reverse course and return to the pre-9/11 culture of hoarding information.

We need to be smarter about how information is shared and appropriately balance security's concerns with the legitimate needs of the users of different types of information. Methods and technologies for doing so already exist. Some of them, I gather, have been put into place since the WikiLeaks case and we need to make sure that we utilize them as fully as possible across our government.

The bottom line is we cannot walk away from the progress we have made that has saved lives. I give you two -- a couple of quick examples.

U.S. Special Forces and elements of the Intelligence community have shared information and worked exceptionally well together in war zones to combat and disrupt terrorist groups such as al-Qaeda in Iraq and the Taliban in Afghanistan. And that would not happen without information sharing.

Here at home, we've used information sharing to enhance the role of state, local, tribal, and private sector entities in our fight against terrorists. And those efforts have paid off, most recently in the case of a chemical supply in North Carolina that alerted the FBI to suspicious purchases by a Saudi Arabian student in Texas who turned out to be building improvised explosive devices. So we need to fix what's broken without going backwards.

Today, I look forward to hearing from each of our witnesses about what they're planning to do to improve the security of classified networks and information while still ensuring that information is shared effectively in the interest of our nation's security. I would also like to hear how Congress can work with you on these efforts either with legislation or through more targeted funding. Efficiently sharing classified information while effectively securing that information is critical to our nation's security and our national values. We can and must have both.

Senator Collins?

COLLINS:

Thank you, Mr. Chairman.

Effective information sharing among federal law enforcement, civilian, and military intelligence agencies is critical to our security. The 9/11 Commission found that the failure to share information across the government crippled efforts to detect and potentially prevent the attacks on September 11, 2001. Improving this communication was a critical part of the Intelligence Reform and Terrorism Prevention Act that Senator Lieberman and I authored in 2004.

The WikiLeaks breach should not prompt a knee-jerk retreat on the sharing of vital information and its use by those analysts who need it to do their jobs. We must not let the astonishing lack of management and technical controls that allowed a private in the Army allegedly to steal some 260,000 classified State Department cables and some 90,000 intelligence reports to send us back to the days before September 11th.

Unfortunately, we continue to see agency cultures that resist sharing information and coordination with their law enforcement and intelligence counterparts. Almost 10 years after 9/11, we still witness mistakes in intelligence oversight reminiscent of criticisms predating our reforms of the intelligence community. Among those cases where the dots were not connected and information was not effectively shared are Abdulmutallab, the so-called Christmas Day bomber, and Nidal Hasan, the Fort Hood shooter.

At the same time, as the Chairman has pointed out, there have been several cases that underscored the incredible value and benefit of information sharing. An example is, as the Chairman has noted, the case of Mr. Zazi, whose plans to bomb the New York City subway system were thwarted.

As such successes remind us, we must not allow the WikiLeaks damage to be magnified twofold. Already, the content of the cables may have compromised our national security. There have been news reports describing the disclosure of these communications as having a chilling effect on our relationships with some of our closest allies. More important, however, they likely have put at risk the lives of some of our citizens, soldiers, and partners.

Longer lasting damage could occur if we allow a culture to re-emerge in which each intelligence entity views itself as a separate enterprise within the U.S. counterterrorism structure, with each attempting to protect what it considers its own intellectual property by not sharing it with other counterterrorism agencies. If those stovepipes reappear or worsen, we will certainly be in more danger.

Such a step backward would run counter to the policy goals embodied in the 2004 Intelligence Reform Act, articulated by law enforcement and intelligence community leadership, and underscored in multiple hearings before this Committee; and that is, to effectively detect and thwart terrorists, the "need to show" must replace the "need to know." The "need to share," I apologize,

must replace the "need to know."

I also would like to hear about the possible technological solutions to the problems that allowed the disclosures to WikiLeaks. For example, my credit card company can detect out-of-the-ordinary charges on my account almost instantaneously. Yet, the military and intelligence communities were apparently unable to detect more than a quarter of a million document downloads in less than two months. Surely, the government can make better use of the technology currently employed by the financial services industry.

It is also notable that the intelligence community was already required to install some audit capabilities in its systems by the 2007 Homeland Security Law, which we authored, which could have included alerts to supervisors of suspicious download activity. Had this kind of security measure been in place, security officers might have detected these massive downloads before they were passed on to Wikileaks.

Technology and innovation ultimately should help protect information from unauthorized disclosure, while facilitating the appropriate sharing of vital data.

I also would like to explore the potential implementation of "role-based" access to secure classified information. Instead of making all information available to anyone who has access to a classified system, under this model information is made available in a targeted manner based on the individuals' positions and the topics for which they are responsible. Access to information not directly relevant to an individual's position or responsibilities would require the approval of a supervisor.

We must craft security solutions for the 21st century and beyond. We live in a world of Tweets and instantly viral videos on YouTube. We must strike the appropriate balance that protects classified and sensitive information while ensuring the effective sharing of vital data. We can use the most cutting-edge technology to protect the traditional tools of statecraft and intelligence - those tools of relationships and information.

Thank you, Mr. Chairman.

LIEBERMAN:

Thank you, Senator Collins, for that thoughtful opening statement.

I want to thank the witnesses before us for coming also, for the thoughtful written testimony you've submitted to the Committee which will, without objection, be included as part of the record.

And now, we'll begin with the Honorable Patrick Kennedy, who's Undersecretary for Management at the Department of State. Welcome, Mr. Kennedy.

KENNEDY:

Thank you very much.

Chairman Lieberman, Ranking Member Collins, Senator Brown, thank you for this opportunity to address information sharing after WikiLeaks and to discuss Executive Branch efforts to ensure that information is shared effectively yet securely in a manner that continues to advance our national security.

The State Department and our interagency partners have long been working to obtain both appropriate information-sharing and protection, and after WikiLeaks, we have focused renewed attention on achieving these dual objectives.

From my perspective, serving over 30 years with the State, both overseas and in Washington, and also serving as the first Deputy Director of National Intelligence for Management, I especially appreciate your efforts to address with us the challenges of information sharing and security.

I can assure you that we at State remain committed to fully sharing our diplomatic reporting within the interagency with safeguards that are reasonable, pragmatic, and responsible.

For diplomatic reporting, the State has historically communicated between Washington and overseas posts through messages which convey internal deliberations relating to our foreign relations and candid assessments of overseas conditions.

This reporting provides State and other U.S. Government agencies crucial information essential to advancing our national interests and we continue to this day to share this reporting through automatic dissemination to over 65 U.S. Government agencies.

In late November 2010, when the press and Wikileaks announced the release of reported State Department cables, we immediately established a 24/7 WikiLeaks Working Group with senior officials, we did suspend SIPRNet access to Net-Centric Diplomacy, the database of state cables while retaining all of our other distribution systems to the other agencies.

We also created a Mitigation Team to address policy, legal, counter-intelligence issues. For continued mitigation efforts both within state and with the interagency, we continue to deploy an automated tool that monitors State's classified network to detect anomalies not otherwise apparent, backed up by a staff who analyze these anomalies.

distribution has been limited to the Joint Worldwide Intelligence Communication System and our traditional system that reaches out, as they said, to 65 agencies. We are now evaluating other systems for distribution such as a searchable database that relies on metadata.

State has continued to work with information management issues with the interagency through an Interagency Policy Committee chaired by the White House Special Adviser for Information Access and Security as well as through existing IPCs.

The challenges grappling with the complexities are threefold. The first is ensuring information sharing policies are consistently directing the use of technology to solve problems, not the other way around. Post-9/11, the focus was on providing technical solutions to information sharing. As a result, technical experts were asked to develop solutions to the barriers. The post-WikiLeaks environment reminds us that technology is a tool to execute solutions but is not in itself the answer.

Simply put, we must more consistently sort out what we need to share before determining how we share it. Connecting systems and networks may provide the means to share information, but we must still manage and share this content in an effective and efficient way, as both of you mentioned in your opening statements.

The national security community must do a better job of articulating what information is appropriate to share with the widest appropriate distribution, and what is more appropriately confined to a narrow audience across the community in order to ensure adequate safeguards.

The State Department believes that the way in which we share messages through our traditional means of dissemination and the steps we have taken since November are leading us firmly in that direction.

The second main challenge involves each agency's rigorous adherence to existing and improved information security policies, as both of you have noted. This includes improved training in the use of labels to indicate appropriate breadth of dissemination. The executive order on classified information establishes the basic levels of classification. From that foundation, individual agencies may still have their own captions that denote how information should be disseminated because not obviously every person with a security clearance needs every piece of worldwide information. Agencies that receive information need to understand how to handle that captioned information, so that it is not inappropriately made available to a too wide an audience.

OMB has directed agencies to address security, counterintelligence, and information issues through special teams. We believe that our Mitigation Team serves as a model for broad, cross-disciplined coordination or governance, because it brings together various subject matter experts.

Many information sharing and security issues can be resolved at the agency level as long as there are standards in place for agencies to execute. For the most part, standards have been created by existing interagency bodies, but there are some areas where further coordination is needed.

The third main challenge involves the coordination, or governance of information management. Numerous interagency groups are wrestling with issues related to the technological aspects such as dealing with standards, data standards, systems, and networks. Others are wrestling with the policy

decisions of who should have access to what classified information. New interagency governance structures to coordinate information sharing have been developed, including those focused, as you rightly note, on sharing with state, local, and tribal governments, as well as foreign partners.

In keeping with the first main challenge, these new structures should maintain or increase focus on defining the content to be shared and protected as well as on the technology which is to be shared and used. Each agency must be confident that the security processes and procedures are applied in a uniform and consistent manner in other organizations. In addition, it must be understood that material originating in one agency will be treated by other agencies in accordance with mutually understood handling instructions.

The State Department shares information with the intent of providing the right people with the right information at the right time. We will continue to share our diplomatic reporting in order to advance our national security information. We recognize the imperative to make diplomatic reporting and analysis available to the entire interagency community. State will continue to do this in order to fulfill our mission. We remain committed to both appropriately sharing and protecting critical national security information.

But this commitment requires, as you've noted, addressing multiple complex issues. We must find the right policies. We must find the right technologies. We must continue to share.

Thank you for this opportunity to appear before you today. I look forward to working with you on these challenges and would be pleased at the right time to respond to any questions you might have.

Thank you.

LIEBERMAN:

Thanks very much, Secretary Kennedy.

Now, we're going to hear from Teresa Takai, Acting Assistant Secretary for Networks and Information Integration, Chief Information Officer, United States Department of Defense.

Welcome.

TAKAI:

Thank you, sir. Thank you for that introduction.

LIEBERMAN:

Thank you. My pleasure.

TAKAI:

Chairman Lieberman, Ranking Member Collins, and Senator Brown, thank you for the invitation to provide testimony on what the Department of Defense is doing to improve the security of its classified networks while ensuring that information is shared effectively.

As noted, I am Terry Takai, and I serve as the principal adviser to the Secretary of Defense for Information Management, Information Technology and Information Assurance. And as such, I'm responsible for the security of the Department's networks and in coordinating the Department's mitigation efforts in response to the WikiLeaks incident.

With me is Mr. Tom Ferguson, the Principal Deputy Undersecretary of Defense for Intelligence. He serves as the principal staff adviser to the Undersecretary of Defense for Intelligence and is responsible for policy and strategic oversight of all DOD intelligence, counter-intelligence and security policy, plans and programs, as delegated by the Undersecretary for Intelligence.

In this capacity, Mr. Ferguson oversees the developments and implementation of the Department's information sharing policies.

The Department immediately began working to address the findings -- Mr. Ferguson and I have submitted a detailed statement for the record, but I would like to briefly highlight a few of the Department's efforts to better protect its sensitive and classified networks and information while ensuring its ability to share critical information with other partners and agencies is continued.

Immediately following the first release of documents on the WikiLeaks website, the Secretary of Defense commissioned two internal DOD studies. The first study directed a review of DOD information security policy. The second study focused on procedures for handling classified information in forward-deployed areas.

Results of the two studies revealed a number of findings, notably that forward-deployed units maintained an over-reliance on removable electronic storage media. Secondly, roles and responsibilities for detecting and dealing with an insider threat needed to be better defined. And finally, limited capability existed to detect and monitor anomalous behavior on classified computer networks.

The Department immediately began working to address the findings and improve its overall security posture to mitigate the possibility of another similar type of disclosure. The most expedient remedy for the vulnerability that led to WikiLeaks was to prevent the ability to remove large amounts of data from the Department secret classified networks using removable medias such as CDs while allowing a small number of computers to retain under strict controls the ability to write removable media for operational reasons.

The Department has completed disabling the write capability on all of its SIPRNet machines

except for approximately 12 percent that maintain that capability for operational reasons, largely in deployed areas of operation. But the machines that maintain write capability are enabled under strict controls such as using designated kiosks with two-person controls.

We're also working actively with National Counterintelligence Executive on its efforts to establish an information technology insider detection capability and an insider threat program. Mr. Ferguson's organization is leading that effort for the Department of Defense and they have been developing comprehensive policy for a DOD CI Insider Threat Program.

In addition, DOD is developing web-enabled information security training that will compliment DOD's mandatory annual information assurance training. And the joint staff is establishing an oversight program that will include inspection of forward-deployed areas.

As DOD continues efforts to improve our information sharing capabilities, we will strive to implement the mechanisms necessary to protect the intelligence information without reverting back to pre- 9/11 stovepipes.

DOD is working closely with its interagency partners, several of whom join me here today to improve intelligence information sharing across the government while ensuring the appropriate protection and safeguards are in place.

I would like to conclude by emphasizing that the Department continues to work towards a resilient information sharing environment that is secured through both technological solutions and comprehensive polices. Mr. Ferguson and I thank the Committee for the opportunity to appear before you today and we look forward to answering your questions.

COLLINS:

Thank you.

Mr. Ferguson, I'm told that you do not have a prepared statement. Is that correct?

FERGUSON:

(OFF-MIKE)

COLLINS:

Thank you.

Before I turn to our next witness, we have been joined by Senator Brown and I just wanted to give him an opportunity for an opening statement, if you would like to have one.

BROWN:

Thank you. I'm actually eager to hear from the witnesses and ask questions. But thank you for the...

COLLINS:

Thank you. And we'll proceed. Our next witness is Corin Stone, who is the Intelligence Community Information Sharing Executive from the Office of the Director of National Intelligence. We welcome you. Please proceed with your testimony.

STONE:

Thank you, Ma'am. Chairman Lieberman, Ranking Member Collins and Senator Brown, thank you for inviting me to appear before you today to discuss the Intelligence Community's progress and challenges in information sharing.

I want to first recognize the committee's leadership on these important issues and thank you for your continued support as we address the many questions associated with the need to share information and the need to protect it.

Your leadership and oversight of information sharing, especially as we come upon the 10-year anniversary of 9/11 has been invaluable. I look forward to our continued participation and partnership on this complex and vitally important issue.

As the Intelligence Community Information Sharing Executive, I am the director's focal point for all intelligence community information sharing matters, providing guidance, oversight and direction on information sharing priorities and initiatives across the community.

In that capacity, I work with -- in coordination with my colleagues at the table and across the community on comprehensive and strategic management information sharing, both internally and with all of our mission partners.

My main focus today concerns information that is derived from intelligence sources and methods or information that is reflected in the analytic judgment and assessment that the intelligence community produces.

I want to be clear though that our concern for the protection of information is not only narrowly focused on sources and methods. As we have seen recently through WikiLeaks, the unauthorized disclosure of classified information has serious implications for the policy and operational aspects of national security.

We all have networks that must be secured. And as technology continues to advance, my colleagues and I remain deeply committed to keeping up with the ongoing challenges we face.

I'm acutely aware that our major task is to find what the Director of National Intelligence has termed the "sweet spot" between the two critical imperative of sharing and protecting information.

Every day, our officers work tirelessly to tackle challenges of increasing complexity in a world that is interconnected, fast paced and ever changing, sharing vital information with each other, customers and partners, leading to better prepared senior policymakers across the executive branch and Congress.

It is important to note that the community's work on these complicated questions predates the recent unauthorized disclosures by WikiLeaks. As you know, the challenges associated with both sharing and protecting intelligence are not new and have been the subject of major effort in the intelligence community for years.

However, these latest unauthorized disclosures underscore the importance of our ongoing and comprehensive efforts to address these evolving challenges. Working within the whole of government to address these issues, the intelligence community's strategy involves three interlocking elements.

The first is access -- ensuring that the right people can discover and have access to the networks and information they need to perform their duties but not to information that they do not need. The second element is technical protection -- technically limiting the ability to misappropriate, manipulate or transfer data especially in large quantities.

And the third area is auditing and monitoring. Taking actions to give the intelligence community day-to-day confidence that the information access granted to our personnel is being properly used.

As we work to both share and protect networks and information, we must never lose sight of the sweet spot. As we continue to increase how much information is shared, we must also increase the protections in place to ensure information is being properly used and safeguarded.

This is the only way to create the necessary trust and confidence in our systems that will foster appropriate information sharing. It's a matter of managing risk, and people, policies, processes and technology all play important interconnected roles in managing that risk.

However, it is also important to note that while all of our capabilities can reduce the likelihood and impact of unauthorized disclosures, in the final analysis, our system is based on trust - trust in the individuals who have access to classified information and trust that they will be responsible stewards of this nation's most sensitive information.

Whether classified information is acquired via a computer system, a classified document or simply heard in a briefing or a meeting, we have had bad apples who have misused this information before and we will unfortunately have them again.

This reality does not mean we should err on the side of not sharing; rather we must put all proper safeguards in place, continue to be forward leaning to find the threat before disclosures occur, be mindful of the risks, and manage those risks with the utmost diligence.

Thank you for the committee's time. And I welcome your questions.

COLLINS:

Thank you. Our final witness on the panel this afternoon is Kshemendra Paul, who is the program manager for Information Sharing Environment of the Office of the Director of National Intelligence.

Welcome, Mr. Paul.

K. PAUL:

Thank you. Chairman Lieberman, Ranking Member Collins, Senator Brown. Thank you for the opportunity to speak about our efforts to effectively share and protect information at every level of government.

Thank you for your attention to information sharing and reform efforts and your support of my office's mission. I also want to recognize my fellow panelists, key partners in government wide efforts to further strengthen information sharing and protection.

As the WikiLeaks story emerged, concerns were voiced that information sharing efforts would suffer a setback. This administration has committed to strengthening both information sharing and information protection. While complex and challenging, we don't see these goals as conflicting. Guidance throughout the executive branch has been consistent. We need to accelerate information sharing in a responsible and secure way.

The WikiLeaks breach is not principally about information sharing and information sharing challenges. A bad actor allegedly violated the trust placed in him. While we cannot always stop bad actors, we can and must take this opportunity to re-assess our posture, our progress and our focus, really, to improving and strengthening information sharing and protection.

The challenges highlighted by the WikiLeaks' breach are complex and go to deeply rooted issues. First, the perpetuation of agency- based bilateral and fragmented solutions versus common and comprehensive approaches to information sharing and protection. Second, the need to protect -- or the need to improve -- excuse me -- improve our counter-intelligence posture, some of the other

technical considerations that my fellow panelist have talked to.

And finally, while the breach involves classified information, we need to be mindful that the root cause issues and the sensitivities extend to sensitive and classified information also, as a whole of government problem, not just a classified national security problem.

I'd like to clarify the information sharing environment and my role. The purpose of the information sharing environment is to improve the sharing of terrorism, homeland security and weapons of mass destruction related information across federal state, local and travel agencies and with our partners in the private sector and internationally.

The information sharing environment spans five communities -- defense, intelligence, homeland security, law enforcement and foreign affairs. It is defined as a cross-cutting, horizontal data-centric trusted information sharing and protection capability.

My role is to plan for -- oversee the agency-based build out and manage the information sharing environment. But my office is not operational. Agencies on the mission, agencies set policies and procedures, and agencies make the investments that interconnect their networks, databases, applications and business processes.

These agency-based contributions, together, form the information sharing environment. The law grants my role, the program manager, government wide authority. This authority is exercised primarily two ways. First, I'm the co-Chair of the White House's Information Sharing and Access Interagency Policy Committee. Through that role, we work through policy and oversight issues. And second, through my partnership with the Office of Management and Budget.

We are being deliberate and collaborative in our pursuit of further strengthening information and protection. We have put an emphasis on governance and outreach. My office, together with my mission partners, is leading the refresh of the 2007 National Strategy for Information Sharing.

We're using this opportunity to leverage common mission equities, to drive common policies and capabilities. And we're orchestrating specific agency-led sharing and protection initiatives with our partners.

We believe this work provides a framework for strengthening efforts to address the root-cause issues associated with the WikiLeaks breach. These capabilities will result in further assuring the proper sharing and protection of information.

Our work across mission partners is profiled in our annual reports to Congress delivered every summer. I also encourage those interested in following or influencing our efforts to visit our website and to participate in upcoming online dialogues and to shaping our future direction.

In closing, our efforts have been and continue to be focused on accelerating information sharing in a secure and responsible way. Effective information sharing and collaboration are absolutely essential to keeping the American people safe.

Thank you for the opportunity to participate in this hearing. I also would appreciate any comments, direction, support or feedback you can provide to me and my office.

My fellow panelists and I look forward to your questions.

COLLINS:

Thank you very much for your testimony and I thank all of the witnesses.

I want to express my personal frustration with this issue. Our committee has held hearings on the lack of information sharing in the case of Abdul Mutalab, where credible information was given to our embassy in Africa but did not make its way to -- in a timely fashion to the National Counterterrorism Center and, thus, Abdul Mutalab was not listed on the no-fly list.

So there's an example of credible information that should have been shared across government but was not. Similarly, in our investigation into the Fort Hood attacks, we found that credible information about Major Hasan's communications with a known terrorist suspect was not shared from the Joint Terrorism Task Force to the Army -- another terrible failure in information sharing.

Now there have been successes as well and there had been many successes. But I mentioned those two failures to share because they contrast and raise such questions with how an Army private allegedly was able to download hundreds of thousands of classified documents and cables and intelligence reports without being detected. And that baffles me.

It also frustrates me because in 2007 Senator Lieberman and I authored Homeland Security legislation that included a requirement that military and intelligence agencies install audit capabilities with robust access controls on classified systems, and those technologies that would enable us to audit information transmission and authenticate identities for access control are not new. They're widely used. And the serious cyber risk associated with the use of removable media devices such as thumb drives have been known for many years.

So my question to all of you is, how did this happen. How could it be that a low level member of the military could download such a volume of documents without it being detected for so long? That truly baffles me.

I don't know who to start with. Mr. Ferguson, do you want to take a crack at that?

FERGUSON:

I'll be the first in the pond. The -- let me take a couple of steps in your questions -- lot of parts to it. The rank of Private Manning is really not so much the issue. It was what his responsibilities were. He was there to provide intelligence support for military operations. So we don't base necessarily on a rank structure. We base it on what is his mission responsibility to support the military. That's number one.

To get to your question about how was he able to access so much data. And then I'll get to the parts about the -- what are we doing and why didn't we do what we could have done kind of thing.

The situation in the theater is such that -- or was -- it's changed now, but we took a risk. It essentially is what it is. We took a risk that by putting information out there, share information to provide agility and flexibility of the military forces there, they would be able to reach in to any of the database in SIPRNet.

They would be able to download that information and they'd be able to move the information using removable media across various domains, in other words, across security domains or from U.S. systems to coalition systems. And we did that so they could do this very rapidly.

Here in CONUS or in the United States, actually, many things you've talked about, about closing off open media ports and so forth actually had been in place for a decade or more. If you go to many of the agencies, they actually are not able to access those open ports. But the focus in the theater was speed and agility.

So we took that risk to allow not just Private Manning, but many people who are serving there to move that at that pace. You asked about why we did not put in place capabilities that was in your bill. In fact as early as '08 we started to deploy what is called Host-Based Security System -- it's what's called HBSS -- as early as '08. And at the time of Private Manning's alleged activities, about 40 percent of the systems in CONUS United States were -- actually had that system in place.

We had systems that were not -- that was not available in the theater.

COLLINS:

And why wasn't it?

FERGUSON:

Maybe because of a lot of the systems there are, for lack of a technical term, cobbled together, and the placing those kinds of systems in there, they're not all equal, sort of family of systems there and it takes -- it's not just like working for Bank of America where they have one homogenous system and they can insert things and take things out as it works.

You have multiple systems and putting a new intrusion software, the monitoring tools and so forth, you have to (inaudible) differently. And that's part of the problem. So, basically, to get away from that and not hold up the ability to move information, they took on the risk of -- by saying, look, the guy -- these people are cleared, they go through background investigations and, frankly, most of our focus was worried about outside intruder threat, not inside intruder -- inside threat.

So, in the end, to answer your question, I'll use my hands here. We had ourselves a situation where we had information sharing at this level and we had put in place -- we took the risk of having monitoring tools and guards and passwords and so forth, as well as people did not fully implement policies, they did not follow security rules down at this level.

So the problem is -- that's where we made our mistake. We allowed this to occur, when we're sharing information at this level. So what we're trying to fix today is not take this level of information sharing and moving it down here, which you have referred to in your opening statement, but take this and move it up here. And that's what we're trying to do as rapidly as we can.

COLLINS:

Thank you. Mr. Kennedy, Mr. Ferguson explained that, basically, DoD in the interest of making sure that the information was out there in theater took a risk, but that doesn't explain to me how the private would have the access to State Department classified cables that had nothing to do with the country for which the private was involved in intelligence activity.

So how did it happen that he had access to cables, State Department classified cables involving countries that had nothing to do with his intelligence responsibility?

KENNEDY:

That's a very good question, Senator. Several years ago, the Department of Defense and the intelligence community came to the State Department and said, we need the State Department -- and actually they paid for it -- to push out reporting to SIPRNet, which is the Department of Defense worldwide system, and to put -- to load a number of our cables on to a Defense Department database that would be accessible to Defense Department people.

So, in response to their request, we took a selected element of our cables and pushed those out to the Department of Defense's database. To be blunt, we believe in the interest of information sharing that it would be a grave mistake and a danger to the national security for the State Department to try to define at each and every one of the 65 agencies that we share our diplomatic reporting analysis to say that Private Smith should get this cable, Lieutenant Jones should get that cable, Commander X should get that cable.

The policies that have been in place between the State Department and other agencies for many years is we provide this information to the other agency. The other agency then takes on the

responsibility of controlling access by their people to these -- to the material that we provide to them.

COLLINS:

I'll come back to that issue, but I want to first give an opportunity for my colleague, Senator Brown, to ask his question.

BROWN:

Thank you. You're in a roll though so.

I've served in the National Guard for 31 years. I'm a lieutenant colonel. I'm, you know, on the computers regularly, all the good stuff. And I have to tell you that sometimes it's like brain surgery getting on the computer, even for somebody like me who's part of the senior staff and, you know, had (inaudible) training just to log on, get access, go where I need to go.

And I still had not really gotten the satisfactory answer as to how this private had a complete and total access to the document he has. I mean, in my wildest dreams, I could not do what he did. And then I say, well, you know, he works 14 hours a day, no one cares. Well, the average work hour and, you know, workload in that region is -- is that and more for many people.

My understanding on doing my own due diligence is that there was a complete break down of command authority when it came to instructing that soldier and people within that command as to the dos and don'ts with regard to information and information sharing. There's no check or balance, and that the amount of people that have access to that information has grown by tens of thousands. Hundreds of thousands of people have access to that information on any given day.

So let me just ask that. Is that accurate that that many people have access to that -- those -- that information and whoever feel qualified to answer it? (Inaudible) do you folks?

(UNKNOWN)

(OFF-MIKE) Thank you. The -- even today, the -- if -- let me put it this way. The SIPRNet is a command and control network is just like the Internet. It has...

(CROSSTALK)

BROWN:

Can you just -- for the purposes -- and I know what that is. I've been in the military. Can you explain to the listeners like what is that?

(UNKNOWN)

What is what -- the SIPRNet?

BROWN:

Yes.

(UNKNOWN)

The SIPRNet is a command and control network that maintains Department of Defense classified secret level information that it covers a whole portfolio of issues. It's not just intelligence information. It's operations data. It's finance formatting data, personnel data. It covers a very large...

(CROSSTALK)

BROWN:

It's everything.

(UNKNOWN)

It's everything. All that information is not available to everyone who's on SIPRNet. A lot of that information in fact is password protected. The -- but there are sites that are just, like going into the Internet, that if you click on there, if you put in a search for that information and it's not password protected, it is available to whomever is on the SIPRNet.

BROWN:

All right. So let me just take what you're saying. But that wasn't the case with this young soldier. We're not just talking about that stuff where you just get online and take that stuff. We're talking about that young person had the ability to not only get that, but all the classified documentation as well. Correct?

(UNKNOWN)

He must have been able get classified information that was not password protected.

BROWN:

Right. Right. And is it true that there are hundreds of thousands of people that have access to that information still?

(UNKNOWN)

That is true.

BROWN:

Once again, I'm not a brain surgeon, but, you know, I am an officer in the United States Military and I have difficulty getting that stuff. Why haven't we like locked down and provided and -- we -- basically, we did improve (ph) the access so that people have access -- number one, to make sure they're all our friends. Number two, where is the command and control in these types of things?

(UNKNOWN)

The command and control, since the -- since the SIPRNet is really a family of networks, the site owners decide, just like on the Internet, who gets access to their particular site.

BROWN:

Right. That's for the open stuff. I'm -- I'm not talking about...

(CROSSTALK)

(UNKNOWN)

No, no, no. That's for -- that's for secured -- secured information as well.

BROWN:

Right. Right.

(UNKNOWN)

So the -- in the case of course of the State Department information, that's now have been removed from SIPRNet. So it's not -- that's not available for everybody to take a look at.

BROWN:

I was kind of surprised they're even on there.

(UNKNOWN)

Well, that was a request of the Department of Defense and the DNI to put that information in

order to make it more accessible to people in the -- in the intelligence community.

BROWN:

Is that -- is the reason why is because there's -- I understand the moving nature of the battle field. Originally -- I mean, I believe that a lot of the command and control went away because of the changing nature of the battle field and then you needed the information very quickly. Is that a fair assessment?

(UNKNOWN)

That is a fair assessment.

BROWN:

So knowing that, what checks and balances have been in place -- put in place? Notwithstanding that fact, what are we doing?

(UNKNOWN)

OK. What they have done isn't -- and Ms. Takai can talk about the -- the technology behind this. But they have put in place when they closed down all the ports so they can't remove the data, but they also have -- they're starting to try to narrow the data access based on mission responsibility for one.

It's not going to be as simple as just going in and turning off stuff and just doing a big survey of the -- of the SIPRNet, although that will probably occur. The -- and then, of course, the moving of the data which was a big concern is now a two-man rule, as Ms. Takai pointed out, about 12 percent of the systems now have -- have the ability to move data and shift it to another domain. The other 88 percent are shutdown.

BROWN:

He used the thumb drive, right?

(UNKNOWN)

He used the CD (inaudible).

(CROSSTALK)

BROWN:

(Inaudible)

(UNKNOWN)

You know, the thumb drives have been shut off for some time.

BROWN:

That's my thought. So it was a CD, right?

(UNKNOWN)

He used the CD. That's right. He was downloading on CDs. The -- so we have a two-man rule. Another key piece of this is -- I don't know what word to use -- we -- a failure on the part to monitor and follow security regulations. It's as simple as that.

BROWN:

No. I understand. I agree with you.

(CROSSTALK)

(UNKNOWN)

(Inaudible)

BROWN:

I know there's protocol in place. And I'm just -- I feel flabbergasted. I mean, here we are. We have one of the biggest leaks in my lifetime, in my memory at least in the military. And, you know, we got a private that's in trouble. What -- what -- I'm a little curious. Like there seems to be -- have been a breakdown completely on the chain of command.

(UNKNOWN)

It didn't work as well as we hoped.

BROWN:

And that being said, it hasn't worked as well as we hoped. Is there anything like a red team or an unannounced inspection or where you changed the protocol?

(UNKNOWN)

Actually, there have been investigations looking at the entire process throughout the entire -- for the entire theater. And a lot of the changes have occurred in terms of the two-man rule, shutting down of the ports and other security -- security training and so forth has all occurred in the last I guess three or four months.

So, yes, they've taken some pretty significant actions already. And if I may, I'd like to pass it to Ms. Takai because she can speak to some of the technologies that are being placed.

BROWN:

And with that -- and then I'll take that testimony in a second, but that being said, I know all the agencies are actually awash with new guidelines and directives. Is there a coordinated effort of some kind being made so that policy and oversight are staying consistent, that agencies are not left to guess like who to listen to?

Is there someone in charge who basically is dictating what we're doing, why we're doing it and how we're doing it and then following up to say, yes, we're in fact doing it, we're good. Is there anything like that doing on?

(UNKNOWN)

There is -- well, yes. Yes, there is -- policies -- I'll give you a good example. We had policies for security and use of material was spread across a number of policy documents. So if you were sitting in a field or here in the United States and you wanted to find where that policy was, you had to go search for it.

In hindsight, that was not a good way of approaching it. It worked that way for years, decades. One of the things we've done is to take all those policies, we've updated those policies and we combined them and consolidated them into a single product. So there's only one place. There's a one-stop shop to go get that. That came out of the Undersecretary of Defense for Intelligence Office. So he sets the guidelines for that information protection, assurance and security parts.

In terms of setting rules for information sharing itself, that is being done as a community-wide activity, not just within the Department of Defense, but with the DNI, with (inaudible) approach and with all the other agencies. So it's -- there's one initiative right now underway and, of course, each department is also looking at it individually.

(UNKNOWN)

Can I amplify that?

BROWN:

Yes, please and then we'll go hear him. I know he has one final statement, but, sure, yes, absolutely.

(UNKNOWN)

So there's an ongoing White House led process right now, look at WikiLeaks incident potential structural reforms. That's got three -- three main tracks that are going on and my -- my panelists and I and others are -- are involved in that process.

The first part of it is looking at how to better balance things like identity management and tagging of information more consistently so you can do better kinds of access controls that we were talking about in the opening statements. The second is looking at the insider threat aspects and some of the technical considerations that we've talked about. And the third is looking at how do we strengthen governance across. So the hope is that in coming weeks and months, we can come back and talk about the results of that process.

BROWN:

(Inaudible).

TAKAI:

Before I start to the technology, just to follow on to the governance issue, there is participation by all the organizations in the White House working group that reports to the deputy's committee around the various activities to make sure that we are well coordinated and that we're working together.

Inside Department of Defense, this is an item that is high on the Secretary's list. And we provide ongoing reports to him from the standpoint of the technology mitigation efforts, both to he and the Chairman of the Joint Chiefs of Staff regarding our progress. So there is significant oversight. There is significant guidance in terms of making sure that we are taking care of this and we are following on to the commitments that we've made both from a technology perspective and working with Mr. Ferguson's area in terms of making sure that the policies are updated.

So I wanted to make sure that I added that in response to the question. Moving on to the technology, I think we've talked about the host-based security system and the progress that we have made thus far in terms of having that installed and making sure that we can detect anomalous behavior in terms of individuals who might get on to the network and download information.

And we're doing that in two ways. One is from a device perspective. The host-based security system detects if in fact the computer does have a device where the information can be downloaded

so that we can validate that and ensure that it is a part of the 12 percent of those computers that we believe need that information in the field.

The second thing that we're doing is to look at what we call an audit extraction module -- to follow on to Senator Collins' question around how do we have the information and the analytics to see where, for those that have that ability, we are seeing anomalous behavior and we can catch it at the time it occurs. We're currently in testing. That software is integrated with HBSS and we will be then moving ahead to roll that out across DOD.

The third thing that we are moving forward on, as you mentioned Senator Collins, is around really a role-based process. We're going to be implementing a PKI identification similar to our current CAC cards that we have on our non-classified network to all of the DOD users. And what that will do is give us an opportunity over time to refine what information individuals have access to.

So sheer access to SIPRNet for instance in this case, we will be able to -- by looking at each individual data base -- take it down to what information that individual needed as opposed to having the network completely open.

BROWN:

I appreciate that. Then just in closing, I -- it was not only dangerous, it's embarrassing what happened. I mean, you know, it's embarrassing for our country some of the things that were actually out there. And so there's a lot of lessons there. But I appreciate the opportunity.

And thank you for having this hearing and participating -- allowing me to participate in it.

COLLINS:

Thank you.

LIBERMAN:

Senator Collins, thanks very much for assuming the Chair. I apologize to the witnesses.

And you're adjourning the hearing now, Senator Brown? That's it. OK.

I appreciate the testimony. Let me ask a few question if I might. In a speech that the DNI General Clapper gave last fall, he predicted that WikiLeaks was going to have a "very chilling effect on the need to share," end quote. After WikiLeaks began to release State Department cables in late November, and news headlines forecasted a clampdown on information sharing. And this is what we've been dealing with and you deal with in your testimony that you submitted.

I wanted to ask you if there are specific areas -- and I guess let's start with Ms. Stone and then the others -- are there specific areas where you think the WikiLeaks case has had a direct impact on information sharing other than the examples cited in the prepared testimony by Mr. Kennedy of the State Department removing its diplomatic cables from SIPRNet?

STONE:

Thank you for that question, Sir. My reaction is that the most direct impact I would say has been in the area of cultural -- culture and those people who are concerned about sharing information, rightly so for the protection matters. And, therefore, our reaction to WikiLeaks must be to increase protection as well as sharing so that as we increase the protection, we also increase the trust and confidence that people have that when they share their information appropriately, it will be protected, we will know where the information is, we will be able to pull that information if it's inappropriately accessed, and we will be able to follow up with appropriate repercussions if and when it is used.

So I think the most direct I have seen is not in a specific tangible action, but more so that it has resulted in a very clear need for us to increase the protection, to increase trust and confidence to share more broadly because we are all agreeing. While Director Clapper was very concerned as we all were that this would have a chilling effect, we've all worked very hard both within DOD and DNI, within the intelligence community and across the government to ensure that it does not have a chilling effect, but, in fact, we -- as Mr. Ferguson said, as we increase sharing, we also increase protection to develop that trust and confidence.

LIEBERMAN:

That's good. Do any of the others -- yes, Mr. Kennedy?

KENNEDY:

If I could, Mr. Chairman, I think there have been two kinds of chilling effects. One I think is there has been a chilling effect on the part of some foreign governments being willing to share information with us. And that is obviously a great concern to the State Department. We build our diplomatic reporting analysis on the basis of trust -- that individuals will tell us things in confidence, we will share them in confidence within the United States government, that it will not go broader than that. So that has been one chilling effect.

I think the State Department though has avoided the chilling effect that you were directly addressing. For example, if I might, during the period of time, we have posted, as you all mentioned, some 250,000 cables to this database posted to the DOD SIPRNet. During that same period of time, we disseminated 2.4 million cables, 10 times as many, through other systems, to other -- the 65 other U.S. government agencies.

And so, therefore, while we stopped disseminating on SIPRNet for the reasons that -- that my

DOD colleagues have outlined, we have continued to disseminate to the intelligence community system, the JWIC System, and we have continued to disseminate the same volume of material to the same other agencies based upon their -- their need for that information.

We do not hold anything back. This unfortunate event has not caused us to hold anything back. We continue to share at the same rate as we were sharing before because we know that our information is essentially the gold standard. There are more reporting and analysis, officers and sources and information from the 265 State Department diplomatic (inaudible) around the world and any other agency (inaudible).

So it is our intent to uphold our piece of national security and obviously to be responsive to the -- to the very, very forceful and correct legislation that you saw passed, which is to share. We are continuing to share using two other means.

LIEBERMAN:

Do any of the other of the three witnesses want to comment either in terms of specific areas of the effect of WikiLeaks on information sharing or perhaps a more indirect impact where the people are becoming more hesitant to work across agency boundaries or even marking intelligence products more restrictively, Mr. Paul?

K. PAUL:

Yes. And in my role, I have the opportunity to work closely with our state and local travel partners. And I just want to report that the concerns about a chilling effect. They share that. They share their concern, but -- and we remain vigilant and we work with them to try to identify any -- any challenges of that sort, but -- but so far, our partners, primarily FBI and DHS, there's a lot of good sharing.

Our different sharing initiatives continue to move forward, things like the Nationwide Suspicious Activity Reporting Initiative, the Nationwide Network of Fusion Centers and different initiatives like those.

LIEBERMAN:

Good. Thanks for your answers to that. Incidentally, one of the things I found and I'm sure other members of Congress have found, in foreign travel that we've done since the WikiLeaks is that, somewhat in jest, but not really, meetings often -- leaders of foreign countries that we're meeting with will say I hope this not going to appear on WikiLeaks.

So they're hoping that there's a certain confidence and trust in the exchange of information. And, of course, we say, no, and then the person from the embassy usually says, no, we've taken care of that problem. But it did leave -- it did affect the trust of allies around the world.

One of the things that Congress called for in the Intelligence Reform and Terrorism Prevention Act was the use of technologies that would allow "role-based access to information in government systems." In other words, that people would have access to information necessary for their work but would not have overly broad access to information that they did not need.

One of the key lessons obviously from WikiLinks is that -- WikiLeaks -- is that we've not yet made enough progress toward that goal as we need to. And if such capabilities had been in place on SIPRNet I presume Private Manning would never have had access to that much information if any at all.

So, I wanted to ask you -- it could be Mr. Paul or Ms. Stone or Ms. Takai, maybe we'll start with you -- what are the key challenges associated with implementing role-based access as I've defined across our classified and sensitive information systems?

TAKAI:

Thank you, Mr. Chairman. I'd like to start first by just giving you by where we stand at DOD in terms of rolling out a PKI- based CAC card for SIPRNet.

LIEBERMAN:

Good.

TAKAI:

We are in the process -- in fact -- are in production if you will to our trusted foundry on those cards. We're anticipating the completion of the roll out by the end of 2012. So, then, all the individuals who today need SIPRNet and use SIPRNet will have PKI identification.

LIEBERMAN:

Have you defined those terms while I was away or would you want to do so now, the PKI and the CAC card for the record?

TAKAI:

Effectively, the Controlled Access Card is a card that you actually utilize with your computer that actually identifies you when you log on to the computer. So, it is a much more sophisticated password, if you will. It gives you a user name and password but it more clearly identifies you. And then, from that, more clearly can identify the role that you play in the organization and then through that the information that you should have access to.

LIEBERMAN:

So, that would all limit access based on what the position of the card holder was and the presumed needs -- needs-to- know of the cardholder.

TAKAI:

That is correct, sir. But to the second part of your question, in terms of our roll out plan --

LIEBERMAN:

Yeah.

TAKAI:

-- and the issues -- they're not issues -- but the steps that we need to go through, the cards are actually rolled out to each individual who has a computer. So, our deployment plan is to actually get the physical cards and the physical readers installed on all of the computers for those individuals that require access to SIPRNet.

Second thing is through the trusted foundry, we have a manufacturing process for those cards and they have a capacity for a certain number of cards. So, that also is a factor.

So, again, in order for us to really complete 100 percent, we have to take into account those two factors, and also the fact that many of the computers where this is needed are, as you could well imagine, in many locations around the globe. And that's not only, of course, certainly on the ground but on ships and so on. So, it will take us a while -- end of 2012 -- to have that deployment complete.

But I think it's important to note in addition to just the physical deployment of the cards and on the various computers that it will then take us additional time to make sure that we get the roles associated with the information connected.

LIEBERMAN:

Right.

TAKAI:

So, the cards give us the capability to do that and then we'll continue the deployment to link the information to that.

LIEBERMAN:

It's encouraging. Thanks. Senator Collins?

COLLINS:

Thank you, Mr. Chairman. And just a couple of more questions. Mr. Ferguson, when I think about the WikiLeaks incident, I think not only of the failures of technology but also of failure to focus on certain red flag behavior that was exhibited by the suspect. And it reminds me very much of what our investigation found when we looked in to Major Hasan's behavior prior to massacre at Fort Hood.

If the media reports are correct, Private Manning exhibited problems such as mental health issues and assaults on colleagues and -- the fact that supervisors had recommended that he not be sent to the front lines.

These are all pretty big red flags. And I'm wondering why they did not lead to a restriction in his access to classified information. I don't know if you're the right person for me to ask that question to. But my point is there is more than just technology at stake here. If we have a high ranking official who -- and we use the user role approach but that individual becomes unstable or embraces Islamic radicalism or there is some other reason that would cause the individual to pose an insider threat. Do we have the systems in place to catch that individual?

FERGUSON:

Senator, I probably can't -- I can't really speak to the specifics of Private Manning while there is an ongoing investigation; however, your point, though, about is there a process to identify behaviors that we should be concerned about and the -- we've taken a look at that. And the training that we had in place, whether it's Hasan or you know this case, was not sufficient to give his supervisors the pieces that they would need to put together and say that this person is a problem and the -- or in some cases, to take action when they did suspect something was wrong.

So, what we have done in the department is begin to shape new policy direction how to better train supervisors, how to best identify behaviors that would be of concern. And also that's one piece. But also be willing to take action and that's part of the other problem. It's not that somebody might say that you with this behavior is irregular, it's also in some cases fear to take action or may reflect on them as a failure or -- and they reflect in some other way. So, there are two hurdles here. It's teaching people how to identify the characteristics. But it's also teaching that the right thing to do is to take action.

COLLINS:

And I am concerned because we've seen two recent cases to where tremendous damage was done despite the fact that there was ample evidence it appears -- I am less familiar with the case we're discussing today -- that something was dramatically wrong. That's an issue I'm eager to pursue. And I think your point about training is a very good one.

Mr. Paul, just for my last question. You mentioned in your testimony that there is fragmented approach to computer security in -- across the federal government. And I think I can speak for the Chairman when I say that we could not agree with you more, and that's one reason we've introduced our cyber security bill which will apply to the civilian agencies and also try to work with the private sector to develop best practices. But our bill does not deal with the intelligence community or the military computer system.

You also in your testimony pointed out that you're not an operational office at DNI and that you're heading a task force on this issue. What are you telling us? Are you telling us that the DNI needs more authority to prevent this fragmented approach where the one intelligence agency may have a totally different approach to security and classification and access than the Department of Defense?

K. PAUL:

So, when I was using the descriptor fragmentation what I was referring to was that agencies put in place specific agency- based solutions. Those solutions serve for specific needs. But then, when you look at more broad information sharing and protection with other agencies, you -- the solutions tend to not work as well.

An example of this is -- as we look at things like identity management frameworks -- some of the panelists have talked about it -- identity management, that's foundational to be being able to do information sharing and information protection. We have several different identity management frameworks across the scope of federal government or state and local partners and so forth.

Those frameworks are mostly aligned. But we need to make sure that as they get implemented, they're implemented in a way that's consistent across all the different partners. If that doesn't happen, then, you run into challenges when information moves across organizational boundaries.

So -- and the second part of your question was about my role in co-chairing the Information Sharing and Access Interagency Policy Committee. A key thing that we're trying to do in that group is to harmonize policy frameworks across the different agencies. To make sure that you know in the one hand, we have a consistent framework; on the other hand, we're not slowing down operational considerations in those agencies. So that the variations that occurred truly because of mission requirements and not because we're not effectively working together.

COLLINS:

Ms. Stone?

STONE:

Thank you. If I could just answer that. Across the intelligence community, we are working very hard to have comprehensive guidelines and processes that are consistent and interoperable.

We have -- we are working on leveraging public key infrastructure and attribute-based access control to be able to have a more comprehensive identity and access management. We're standardizing data protection models to have several models of security and we're working on an enterprise audit framework.

So, within the intelligence community, while we may have different systems, we are working very hard from the Office of the Director of National Intelligence to more standardized and make -- ensure consistency across those networks.

The way we then plug in with the rest of the government -- and, indeed, we must interoperable with the rest of the government, of course -- is through this interagency group that we are working on, together with everyone at the table and others, to ensure that we can in fact be coordinating and consistent with the other offices and we're still working through exactly what that looks like. But that is certainly a concern that we're all very well aware of.

COLLINS:

Thank you. And just a final concluding comment, I would note that the JAO continues to list the information sharing of -- particularly with regards to terrorism-related information as a high risk activity and it is on the high risk list again this year. And finally as we look at the use role approach which I brought up in my opening statement -- and which we've commented on today -- we do have to be careful that that does not translate back to the bad old days where no one shared anything and where we have the stovepipes because we're defining who has access so narrowly that we deny access to analysts who really need that information. So, it's a very difficult task you're all embarking on.

But in this day and age that an individual could have -- be able to undetected for so long download and illegally distribute hundreds of thousands of important tables and reports and documents is just inconceivable to me. So, clearly we have a long way to go to strike the right balance. Thank you, Mister Chairman.

(UNKNOWN)

Thanks very much, Senator.

LIEBERMAN:

Thank you, Senator Collins, very much. Thanks again for taking the chair while I had to leave. Just a few more questions. I want follow up first with one to you, Mr. Paul, following up on the question I asked Ms. Takai before about role-based access.

In your testimony, you note the fact that there are "At least five distinct identity credential and access management frameworks in use by federal agencies." And, of course, that makes me wonder

whether that limits the ability to implement the kind of role-based access capabilities that the (inaudible) required in systems in the cost-effective way. I wonder if you could talk about what you are doing -- hopefully, in cooperation perhaps with the other witnesses here today -- to harmonize those different access frameworks?

K. PAUL:

Sure. Thank you for the question. There are at least five different frameworks but they're really not that different. They are different enough, though, that it requires the attention of my office and other bodies, the Federal CIO Council, for example and my colleagues here to make sure that these - - as the frameworks get implemented in the different agencies and with our state's local travel partners, that we don't allow for variations, where the variations are controlled -- right -- and reflect mission requirements and the like.

So, a focus of my office is to work with the interagency bringing together groups to make sure that as these frameworks get implemented, they are implemented in the consistent way. Building on top of that, it's critical that as we look at role and attribute-based access controls that you both have highlighted, there's a framework for doing those -- how we define roles, how we -- and to use a colloquial -- we tag data, we tag people. That tagging occurs in different places. A person may be tagged in one agency then he may be tagged in another.

We wanted to be able to have that data moved in an appropriate with policy enforcement. That means there needs to be a consistent framework for how that happens, right, and the coordination. And -- and this goes to some of what you've heard from -- from me and others about the importance of governance of the standards and architectural approach and -- and things like that.

So, those are contributions that are catalyzed through the efforts of my office with close cooperation with my mission partners.

LIEBERMAN:

Good (inaudible) on that.

Mr. Ferguson, maybe Ms. Takai, while I mentioned in my opening statement the great successes that we've had in the past few years in Iraq and Afghanistan in disrupting terrorist networks in those countries where the military and intelligence working are very closely together and being so in a remarkably rapid way, sometimes exploiting information from one lead or one source and using it within an hour elsewhere.

As you make -- or quicker (ph) -- as you make changes to improve the security of classified networks at DOD and in the intelligence community, are you taking steps to ensure that those efforts won't diminish or slow down our ability to carry out the kinds of operations I've just described?

FERGUSON:

Yes, sir, absolutely. One of the -- even though the process was to allow personnel working in a secured facility to access the SIPRNet and pull down data and copy it through open media.

LIEBERMAN:

Right.

FERGUSON:

For example, sir, we have more (inaudible) flexibility. We've gone back and taken a look at how that process worked. And we have found that by creating it is a kiosk process and a two-man rule. We can still move at the same speed and have the same agility without giving everybody the same availability to the information and being able to pull the data down and copy it.

So, very much in mind to make sure that we do not hinder our ability to carry out.

LIEBERMAN:

You want to add anything, Ms. Takai?

TAKAI:

Yes, I would. I think one of the things that's very important is that we continue to see the dramatic need for information and information sharing by the war fighter. And so, if anything, the demand for that information continues to grow.

And so as we're looking at the technology just to relate back to what Mr. Paul said, part of our efforts are to ensure within DOD we are eliminating our fragmented environment which has grown up over time through our legacy base of the way our networks have grown up, by the way that our databases have grown up.

And so I wanted to make sure that I added that there was a relationship between the work that Mr. Paul's doing, the work that we're doing internal to DOD. And I'm sure my partners here are all undergoing the same thing that it's really what Ms. Stone was talking about.

And those things in combination with being able to apply cyber security enhancements are really going to give us an opportunity to get that information out there as quickly as today, and in some cases, even faster than today, but to do it in a secure way.

LIEBERMAN:

Excellent.

Let me ask a final question, based on the testimony you've provided about really what you're doing to respond to the challenge -- challenges that were illuminated by the WikiLeaks case, but also to protect the information sharing environment.

One, have you seen any areas where you think you would benefit from statutory changes? And, two, this is a question that I ask in a limited way in this fiscal environment. Are there any funds we should be targeting to particular users that we're) not now to assist you in responding to this crisis?

Maybe we'll start with Mr. Kennedy, go down the row if anybody has anything to say.

KENNEDY:

Thank you very much, Mr. Chairman.

I can't think of any additional legislative authority. I think you've done two things. You've given us the intent.

LIEBERMAN:

Right.

KENNEDY:

And then you've given us the command. And I think we know, from what you've said and what we know internally, which ways we should go. On the funding, I mean I can always say that we could use -- an institution as small as State Department can always use additional funding given the range of demands.

But I believe that we have systems in place. We have a role-base access system in place that we use to distribute material within the State Department. If you're on the French desk, you'll get one set of material. If you're on the Japan desk, you get another.

And we believe we also have the ability to -- and as I've mentioned earlier, we will continue to push State Department reporting to other agencies. But it does -- I'll admit -- put a burden on them...

LIEBERMAN:

Right.

KENNEDY:

To then take our material which we have provided to secretary of Defense so to speak, to DOD, and then to -- to distribute that to their people according to the roles that -- that only they are capable of defining because it, I think, would be wrong for me to say, which individuals within an entity as large as the Defense department or as large as the DNI or the intelligence community, which analyst needs what.

So, we send it to them and I think they -- they may be the ones who -- who have to answer that second question about how they're going to distribute it efficiently and effectively as -- as both you and Senator Collins have talked about.

LIEBERMAN:

OK, thanks.

Ms. Takai, any legislative recommendations or budget targeting?

TAKAI:

In terms of the legislative question, I agree with Mr. Kennedy. At this time, we do not see any additional legislation that we need. We are going through a review with the -- to answer exactly that same question for the secretary in terms of, is there any need for any change not only additional funding but a change in the cadence of the funding. And so once we have that pulled together, we'd be happy to share it with you.

LIEBERMAN:

Appreciate it.

Mr. Ferguson?

FERGUSON:

I'd have to agree on the legislative side. And certainly, as Ms. Takai has pointed out, as we go through this process, putting in these capabilities, what kind of funding needs, I guess we need to identify what those real costs are and come back.

LIEBERMAN:

OK.

Ms. Stone?

STONE:

Similarly on the legislative, I think we -- we probably got what we need for now although I would reserve the right to come back if we discover we need something else.

And on the funding piece, I think, again, we do have an interagency process ongoing looking at exactly what we might do with different options. So, we'd have to see where that comes out. But I do believe there's at least something in the F.Y. '12 proposal submitted by the President to -- to work on some of these issues.

LIEBERMAN:

Good.

Mr. Paul?

K. PAUL:

Let me just echo Ambassador Kennedy. The laws that this committee -- the -- the statutes that this committee has championed provide an adequate basis, a fine basis. I know in the context of the information sharing environment that it's my responsibility. There's enough authority that's been issued for me now of execution and leadership.

LIEBERMAN:

Good.

Thank you, all.

Senator Collins?

COLLINS:

Thank you.

LIEBERMAN:

Well, thanks very much for, again, your prepared testimony and the oral testimony. And I emerge encouraged that you're certainly dealing with the specific series of vulnerabilities that the WikiLeaks

Manning case revealed.

And I presume in the nature of the modern world with technology and innovation and exploitation, whatever it is, you'll also be thinking about the next way in which somebody might try to take advantage of our information sharing environment.

But I -- I think we've raised our guard in a sensible way and also continue to share information is what I take away in which we need to do from this hearing and I appreciate that very much. The record will remain open for 15 days for any additional questions or statements.

With that, the hearing is adjourned.

CQ Transcriptions, March 10, 2011

List of Panel Members and Witnesses

PANEL MEMBERS:

SEN. JOSEPH I. LIEBERMAN, I-CONN. CHAIRMAN

SEN. CARL LEVIN, D-MICH.

SEN. DANIEL K. AKAKA, D-HAWAII

SEN. THOMAS R. CARPER, D-DEL.

SEN. MARK PRYOR, D-ARK.

SEN. MARY L. LANDRIEU, D-LA.

SEN. CLAIRE MCCASKILL, D-MO.

SEN. JON TESTER, D-MONT.

SEN. MARK BEGICH, D-ALASKA

SEN. SUSAN COLLINS, R-MAINE RANKING MEMBER

SEN. TOM COBURN, R-OKLA.

SEN. SCOTT P. BROWN, R-MASS.

SEN. JOHN MCCAIN, R-ARIZ.

SEN. JOHN ENSIGN, R-NEV.

SEN. ROB PORTMAN, R-OHIO

SEN. RAND PAUL, R-KY.

SEN. RON JOHNSON, R-WIS.

WITNESSES:

PATRICK F. KENNEDY, UNDER SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT OF STATE

TERESA M. TAKAI, CHIEF INFORMATION OFFICER, ACTING ASSISTANT SECRETARY FOR NETWORKS AND INFORMATION INTEGRATION, U.S. DEPARTMENT OF DEFENSE

THOMAS A. FERGUSON, PRINCIPAL DEPUTY UNDER SECRETARY FOR INTELLIGENCE, U.S. DEPARTMENT OF DEFENSE

CORIN R. STONE, INTELLIGENCE COMMUNITY INFORMATION SHARING EXECUTIVE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

KSHEMENDRA PAUL, PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Source: **CQ Transcriptions**

All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of CQ Transcriptions. You may not alter or remove any trademark, copyright or other notice from copies of the content.

© 2011 CQ Roll Call All Rights Reserved.