Enhancing Cybersecurity in a World of Real-Time Threats: Insights from Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security

By Michael J. Keegan

As a nation, we are faced with pervasive cyber threats. Malicious actors, including those at nation-state level, are motivated by a variety of reasons that include espionage, political and ideological beliefs, and financial gain.

The U.S. Department of Homeland Security (DHS) and its National Protection and Programs Directorate works to assist federal agencies to understand and manage cyber risk, reduce the frequency and impact of cyber incidents, readily identify network security issues and take prioritized action. What are DHS's key cybersecurity and communications priorities? What is the mission of the National Cybersecurity and Communications Integration Center (NCCIC)? How is DHS building capacity to accelerate the sharing of cyber threats? Dr. Phyllis Schneck, deputy under secretary, Cybersecurity and Communications, National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security, joined me on *The Business of Government Hour* to provide her insights into these questions and much more. The following is an edited excerpt of our discussion, complemented with additional research.

Before we delve into specific initiatives, perhaps you could outline the mission and continuing evolution of the U.S. Department of Homeland Security's National Protection and Programs Directorate (NPPD)? What roles does your office play in achieving the directorate's mission in support of the department?

Dr. Phyllis Schneck: The mission of DHS's NPPD is to lead the national effort to secure and enhance the resilience of the nation's infrastructure against cyber and physical threats. This is very important, because we must look at all threats and their potential consequences. When something happens, we may not know if it is a cyber or a kinetic event, but we have to be ready to mitigate either threat. This requires that we be prepared. We have to know who to call. We have to understand the specific sector, whether it is water, electricity, or communications. NPPD leads the national effort to do just that—to protect and enhance the resilience of the nation's physical and cyber infrastructure. Its ultimate goal is to advance the DHS's national security mission by reducing and eliminating threats to the nation's critical physical and cyber infrastructure. It does this with the assistance of the following components that compose the National Protection and Programs Directorate, led by my boss, under secretary Suzanne E. Spaulding: Federal Protective Service (FPS); Office of Cyber and Infrastructure Analysis (OCIA); Office of Infrastructure Protection (IP); Office of Biometric Identity Management; and the Office of Cybersecurity and Communications (CS&C).

Within the NPPD, I lead the Office of Cybersecurity and Communications, which is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center, and as a national point of cyber and communications incident integration.

"Whether it is the Einstein Program, the Continuous Diagnostics and Mitigation, or NCCI, it's all about forging and sustaining partnerships. It is about people talking to people, sharing science and knowledge, and building relationships, so when something happens, we know who to call and what to do. If you can't connect, you can't share information and that is what we're protecting, our connections and our way of life."

What are your specific responsibilities as deputy under secretary for cybersecurity and communications?

Dr. Phyllis Schneck: It is a long title with multiple responsibilities. I am deputy for cybersecurity and communications to the under secretary of the NPPD, Suzanne Spaulding. I am the chief cybersecurity official for the department and support its mission of strengthening the security and resilience of the nation's critical infrastructure. This involves making sure that our cyber mission is always fully integrated into the under secretary's vision of how to enhance our resilience against physical and cyber threats. Secondly, I also oversee the entire cybersecurity and communications operation. Whether it is the Einstein Program, the Continuous Diagnostics and Mitigation, or the National Cybersecurity and Communications Integration Center (NCCI), it's all about forging and sustaining partnerships. It is about people talking to people, sharing science and knowledge, and building relationships, so when something happens, we know who to call and what to do.

If you can't connect, you can't share information and that is what we're protecting, our connections and our way of life. All of this comes under my purview, as well as understanding how we work with the cyber mission in each of the components that comprise DHS.

Given the critical mission of your office, what are the top challenges that you face in your position and how are you addressing these challenges?

Dr. Phyllis Schneck: Well, the challenges faced are linked to my priorities. I'll try to distill them accordingly, so you can get a sense of both the challenge and priority being pursued to address it.

- **Building Trust.** Number one is building trust with all of our stakeholders. My first priority therein for those stakeholders/customers is building their trust so they share with us information about cyber events. Every time we learn something about a cyber event, we can use that information to protect others. Gaining such trust is also a challenge in this environment. I hear from my private sector colleagues and I know from my experience, there has never been a harder time to share information or even, in some cases internationally, be affiliated with the U.S. government as a private company. But there has also never been a more urgent time to put information and knowledge together, to connect the dots, to have that resilience in our infrastructures, both cyber and physical. Building that trust is both a top priority, and a significant challenge for me.

- **Building Situational Awareness.** My second priority and challenge involves building situational awareness—that means every time we protect something, we should learn from that event, and use that information to protect, mitigate, and respond to events as quickly as possible. Again, I can flip that and say that's an enormous challenge. We are widely interconnected. We face an adversary that has plenty of money and no lawyers. They have absolutely nothing to protect and they execute with amazing alacrity. We are building that same alacrity. We have to overcome the asymmetry. If we don't protect our privacy, civil liberties, and infrastructure, then we are not in the right business. Building situation awareness is both a priority and a challenge.

- **Leveraging the Cybersecurity Framework.** My third priority and challenge centers on leveraging the cybersecurity framework called for in Executive Order 13636 and developed in 2014 by the National Institute of Standards and Technology (NIST). The Executive Order called for the development of a voluntary risk-based Cybersecurity Framework, a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses. The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. It is my priority and challenge to take the subject of cybersecurity once and for all into the boardroom. Cybersecurity demands the attention of senior leadership to understand the potential risks and consequences, so that they can invest properly in defending their resources and infrastructure. The cybersecurity framework has helped us get the message out where it matters and in a form that is compelling to both private and public sector leaders.

“The “weather map” initiative aims to apply to cybersecurity threats what the National Weather Service analysts do to predict climate conditions. Tornadoes happen fast. Cyber happens faster. The goal is to get a full-scale, real-time model of the potential cyber threat agencies face. This effort is in the early stages.”

Would you tell us more about the “weather map” approach to predicting cyber threats that you are pursuing?

Dr. Phyllis Schneck: This is one of my favorite topics. I studied high-speed tornado forecasting with high performance computing before I entered cybersecurity. Everybody can picture a weather map. You probably looked at one this morning. It will show you detailed weather information in near real-time. You don’t need detailed information on upper atmospheric behavior. You just need to know if it’s going to rain and if you’re going to wear a hat. That’s very much what we need in cybersecurity. Let me illustrate: A colleague who grew up in the Midwest would run for cover when the sky turned yellow—the sky turning yellow is the indicator. Meteorologically, frozen dirt may be in the upper atmosphere. In the summer, if you’re seeing an indication of freezing and you have really hot air below, convective behavior manifests, thus leading to bad storms.

The “weather map” initiative aims to apply to cybersecurity threats what the National Weather Service analysts do to predict climate conditions. Tornadoes happen fast. Cyber happens faster. The goal is to get a full-scale, real-time model of the potential cyber threat agencies face. This effort is in the early stages.

Would you tell us more about the mission and purpose of the DHS’s National Cybersecurity and Communications Integration Center (NCCIC)? How does it foster the coordination and integration of cyber situational awareness and incident management?

Dr. Phyllis Schneck: Our National Cybersecurity and Communications Integration Center (NCCIC) is core to all of our efforts. The NCCIC mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation’s critical information technology and communications networks. Thus, it’s the heart and soul of fostering that rapid information sharing. It serves as a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for federal government, the intelligence community, and law enforcement. The NCCIC shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Let me put that into some “non-Klingon” for fun: It means the raw materials of cyber threat indication. So, not a social security number, not your name, not what you ate that day, but really machine readable, executable code that would indicate that this code is going to do something to your machine, such as tell it to talk to others or share things with others when it shouldn’t. In 2014, the NCCIC received over 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams also detected over 64,000 significant vulnerabilities on federal and non-federal systems and directly responded to 115 significant cyber incidents.

At DHS, we are uniquely positioned as a civilian agency with the only statutory privacy officer in civilian government to work directly with experts in privacy and civil liberties, so that in this time where it is so hard to bring a lot of extremely urgent information together, we can do that. That is our job in the NCCIC. It is also important to point out that we have been doing this “near real-time” or very fast. The NCCIC actively shares cyber-threat indicators to and from multiple sources including private sector partners, the intelligence community, federal departments and agencies, law enforcement, state, local, tribal and territorial governments, and international governments. This sharing, which has been taking place for many years, takes many forms, including person-to-person interactions on the NCCIC floor, manual exchange of information via e-mail and secure web portals, and more recently via automated, machine-to-machine exchanges in STIX and TAXII protocols. While all of these sharing methods have value, the cybersecurity community has recognized the strategic importance of migrating cyber-threat indicator sharing to more automated mechanisms when and where appropriate.

Given your experience in both the private and public sectors, how would you compare and contrast the management and leadership traits and characteristics needed to address the unique challenges faced?

Dr. Phyllis Schneck: In the private sector, we are driven by quarterly performance: your bottom line is money. Your money comes from doing a mission. In government, every day our bottom line is our mission and we simply need money to support it. So it's a little bit flipped. As a leader, it's all about people. Our mission is hard, but it is doable. People love a challenge. We're driven by the ability to make a real difference and a real impact in this area. We want to hire the best and the brightest and to me, as a leader, that's what is most important right now for us to be successful and achieve our mission. ▫

To learn more about the U.S. Department of Homeland Security, go to www.dhs.gov/office-cybersecurity-and-communications.

To hear *The Business of Government Hour* interview with Dr. Phyllis Schneck, go to the Center's website at www.businessofgovernment.org.

To download the show as a podcast on your computer or MP3 player, from the Center's website at www.businessofgovernment.org, right click on an audio segment, select Save Target As, and save the file.

To read the full transcript of *The Business of Government Hour* interview with Dr. Phyllis Schneck, visit the Center's website at www.businessofgovernment.org.