Prepared Testimony and Statement for the Record of

Frank Dimina
Area Vice President, Federal
Splunk Inc.

Hearing on "CDM, The Future of Federal Cybersecurity?"

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

January 17, 2018

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee:

Thank you for the opportunity to appear before the subcommittee to discuss the Continuous Diagnostics and Mitigation (CDM) program at the Department of Homeland Security (DHS).

My name is Frank Dimina, and I serve as the Area Vice President, Federal for Splunk Inc. In this role, I oversee Splunk's federal civilian government business. I originally joined Splunk as the director of the homeland security and law enforcement team. During my tenure at Splunk, I have worked with federal agencies, including DHS, on multiple cybersecurity and data analytics projects. My entire 20-year career has been within the cybersecurity industry, including several years as a Security Operations Center director and as a cybersecurity consultant providing advisory services and incident response support to public sector and commercial organizations.

Splunk is a fast-growing software company based in San Francisco with a singular mission: make machine data accessible, usable, and valuable to everyone. Machine data is produced by every digital device, including computers, mobile devices, networks, sensors, software applications, and many other sources. Machine data contains valuable information that is used for security, anti-fraud, IT operations, compliance, business analytics, internet of things (IoT), and other use cases. More than 13,000 companies, government agencies, universities, and other organizations are using the Splunk software platform. In the cybersecurity area, Splunk's software platform often serves as the nerve center of an organization's security operation center, providing a single pane of glass view for security analysts across an organization's entire security posture. Many federal agencies, including DHS, currently use Splunk.

Before I proceed with the rest of my testimony, I would like to recognize this subcommittee's leadership on the issue of cybersecurity. Cybersecurity is a rapidly changing landscape, with threat actors and technology providers evolving daily. Legislation and robust congressional oversight will be critical as we all work in partnership to strengthen cybersecurity on a national, state, local, enterprise, and consumer level.

In my testimony today, I will provide my views on three main topics:

- The progress to date of the CDM program;
- Opportunities to modernize and enhance the CDM program; and
- Supporting CDM's continued success over the next several years.

Progress of the CDM Program

The CDM program, which was established by Congress to provide risk-based and cost-effective cybersecurity across the federal government, has made significant progress over the last several years. Through the CDM program, DHS has taken significant steps to provide federal agencies with capabilities and technologies that identify cybersecurity risks on an ongoing basis, prioritize those risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant threats first.

This progress is due to the dedication and hard work of the CDM team at DHS and the support that the program has received from Congress and DHS leadership. CDM has raised the bar for security and provides a solid foundation for achieving a baseline of protection across the federal IT landscape.

Members of the Splunk team have been involved with CDM from the very beginning of the program. Currently, Splunk software is deployed as a part of the CDM program at all twenty-four civilian CFO Act agencies. We have witnessed both the early challenges and the more recent steady and consistent implementation of CDM across federal agencies. Since the beginning, Splunk has worked with various system integrators supporting the CDM program. That viewpoint has given us unique insights into the operational challenges, successes, and needs of the program.

A critical decision made during the genesis of the CDM program was the adoption of a phased approach. Phase 1 of CDM, which is focused on determining what is on the network, has helped federal agencies to identify the endpoints on their networks and raise awareness of the extent of their cyber footprint. After deploying phase 1 tools, some federal agencies found a significant number of additional endpoints within their enterprise. As a result, those agencies are now carrying out efforts to bring those endpoints into the program.

Phase 2, which focuses on determining who is on the network, is just now rolling into production. We believe the goal of phase 2, building a master user record for users of federal networks, will be essential to threat mitigation and risk awareness across the federal government.

DHS and the General Services Administration (GSA) are in the process of procuring CDM phase 3 and phase 4, which focus on determining what is happening on the network, via the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) Task Order series. Once fully implemented, phases 3 and 4 will give federal agencies the ability to move from legacy, time-based system accreditation to dynamic, risk-based, and event-driven authorization. This will vastly improve the security posture of the federal cyber landscape.

Modernizing and Enhancing CDM

Building on the progress to date, I believe that there are important opportunities to further modernize and enhance the CDM program. One key opportunity is to better leverage the existing data collected throughout CDM.

In our view, DHS should enhance the existing CDM integration layer so it becomes a common data analytics fabric that is standardized across the program. The data analytics fabric would serve as a platform for collecting security-relevant data across federal agencies at scale, which would enable DHS to perform flexible search queries, build robust visualizations, and provide real-time reporting of the results. There are several key benefits to this approach.

First, a common data analytics fabric would improve the granularity of data available to federal cyber analysts. Today, CDM data presented in the federal dashboard is summary data. Like a photograph, summary data provides a snapshot in time, but lacks the fidelity of a live video feed. Providing DHS analysts with greater detail and drill-down capability would significantly enhance their ability to proactively hunt for malicious activity.

Second, a common data analytics fabric would provide DHS and security teams at federal agencies with drill-down access to granular data at machine speed. Across the government, there is a clear need for real-time access to cyber data from the analyst up to the executive. Moving this access to machine speed will strengthen the effectiveness of the government's response to attacks against federal systems.

Third, a common data analytics fabric would provide the foundation to integrate CDM data with security data from other shared service initiatives like EINSTEIN, the DHS program that provides perimeter defense for federal agencies. Allowing the analysts at DHS to correlate EINSTEIN and CDM data would be an important step as it would provide a level of visibility that is not possible today.

The approach I have described would enhance efficiencies in cybersecurity and information sharing within DHS and between DHS and agency partners. It might also result in additional economic benefits for the federal government by standardizing CDM components, reducing human capital expenditures, and enabling operational efficiencies across CDM.

Supporting CDM's Continued Success over the Next Several Years

Promoting CDM's continued success over the next several years will require continued funding through appropriations, robust oversight by Congress, and sustained leadership from DHS.

Success also requires a smart acquisition strategy that is flexible and encourages participation by innovative cybersecurity companies. One positive step is the decision by DHS and GSA to move to the GSA Special Item Number (SIN), reflecting lessons learned from the procurements associated with the CDM Blanket Purchase Agreement (BPA). This change instills a flexible approach that allows for CDM technical capabilities to evolve through the Request For Services (RFS) model. We believe the continued adoption of this acquisition strategy will help to keep CDM agile, innovative, and competitive.

Thoughtful design of the next phase of CDM will help DHS to better position the program for the future. CDM must be able to evolve quickly and allow for additions of new technologies that can enable risk-based monitoring and protection for modern practices such as cloud and micro-services.

The future of the CDM program has critical implications for the security and resilience of the federal government's infrastructure. CDM can also set a positive example for large organizations outside of the government, since some of the key concepts of the CDM program have applicability in the private sector.

Conclusion

In closing, I will reiterate that the CDM program has made important strides. Now is the time to look at modernizing the approach and enhancing the capabilities of this program.

We look forward to our continued role in the government-industry partnership that will move CDM forward to the next level.

Thank you for the opportunity to testify before you today. I look forward to answering any questions you might have.