dlt.com

REPORT

Civilian Market Analysis

DHS Strategic Industry Conversation

Louis Dorsey
Senior Director, Civilian Strategic Markets

DLT®

Accelerating Public Sector Growth for Technology Companies

November 2018

DHS Strategic Industry Conversation

Nov 1, 2018

Soraya Correa, DHS Chief Procurement Officer

Claire Grady, DHS Acting Deputy Secretary

Civilian Market Analysis

Some of the mission-focused topics discussed by these DHS leaders included:

Keynote Address

- *Claire Grady, DHS, Acting Deputy Secretary*

Lessons Learned from an Unprecedented Disaster Season

- *Brock Long, FEMA, Administrator*

DHS Leadership Insights on Challenges Confronting DHS

- *Kathleen Fox, FEMA, Assistant Administrator*
- *Jeanette Manfra, CISA, Assistant Secretary*
- *Robert Perez, CBP, Deputy Commissioner*
- *Patricia Cogswell, TSA, Deputy Administrator*

DHS Security Operations Center Optimization—Crawl Phase

- *Paul Backman, DHS, CISO*
- *Alma Cole, CBP, CISO*
- *Kevin Graber, USSS, CISO*
- *Vu Nguyen, Cyber Operations, Director*
- *Rob Thorne, ICE, CISO*

How Management Directorate is Enabling the Mission

- *Chip Fulghum, DHS, Deputy Under Secretary for Management*

CXO Partnerships: Addressing the Needs of Tomorrow

- *Chip Fulghum (Moderator)*
- *Soraya Correa, DHS, Chief Procurement Officer*
- *Tom Chaleki, DHS, Chief Readiness Officer*
- *Debra Cox, Office of Program Accountability & Risk Management, Executive Director*
- *Roland Edwards, DHS, Deputy Chief Human Capital Officer*
- *Stacy Marcott, DHS, Acting Chief Financial Officer*
- *Richard McComb, DHS, Chief Security Officer*
- *Dr. John Zangardi, DHS, CIO*

Unity of Effort: Driving Mission through Information Technology

- *Dr. John Zangardi (Moderator)*
- *Michael Brown, ICE, CIO*
- *Dave Epperson, CISA, CIO*
- *Shawn Hughes, EIS Program Management Office, Director*
- *Bill McElhaney, USCIS, CIO*
- *Donna Roy, Information Sharing & Services Office, Executive Director*

Chip Fulghum, DHS Deputy Under Secretary for Management

Dr. John Zangardi, DHS Chief Information Officer

Paul Beckman, DHS Chief Information Security Officer

Keynote Address: Claire Grady

Serving as the Under Secretary for Management (USM) since August 2017, Claire Grady is the third-in-command of the Department of Homeland Security. She is responsible for all aspects of the DHS management programs that support homeland security operations, including financial management, human capital, information technology, procurement, security, and asset management.

> **"DHS operates in a no-fail environment."**

One of her biggest concerns is not the threats of today, but the threats of tomorrow. DHS is seeing emerging threats outpacing our businesses which is unacceptable. As an example, Grady spoke about the use of unmanned systems (drones) used by terrorists on the battlefield to destroy, drug smugglers using drones to monitor border patrol routines in order to get inside the U.S., and criminals using drone technology to get inside sensitive areas. She was emphatic on working together with industry to get ahead and counter these types of threats.

Session I: DHS Leadership Insights on Challenges Confronting DHS

Kathleen Fox, Assistant Administrator for FEMA, discussed the steady-state operations of FEMA and how her team helps with preparedness for disaster events. Part of that involves helping FEMA teams plan true National Incident Management System (NIMS) guidance. Today's NIMS is provided in a pdf format so it is not very sophisticated. Fox is looking for industry's help to provide more innovative and modernized approaches to this process. FEMA also needs industry help in firming what their emergency and financial preparedness message to those 50 percent of Americans that are not financially prepared for emergency disasters. As an example, she provided that with Hurricane Harvey last year, a large proportion of people in Houston did not have flood insurance.

Jeanette Manfra is the Assistant Secretary for Cybersecurity and Infrastructure Security Agency (CISA). As the chief cyber official, she runs the cybersecurity effort for defending today and securing tomorrow. Manfra's primary focus is on the evolution of terrorists and nation-state actors using cyber means to hold U.S. critical infrastructure at risk.

The President signed into law the Cybersecurity and Infrastructure Security Agency Act on November 16, 2018 which elevated the mission of the formally known National Protection and vectorate (NPPD) within DHS and established the now Cybersecurity and Infrastructure Security Agency (CISA). Manfra discussed CISA's two primary missions, (1) Federal Civilian Cybersecurity and (2) Critical Infrastructure. Manfra pointed out that The Federal Information

Security Management Act (FISMA) states that every agency is responsible for their cybersecurity; Office of Management and Budget (OMB) is responsible for issuing policies; Department of Homeland Security (DHS) is sort of in the middle by helping agencies implement guidance and providing capabilities. CISA has the authority to mandate agencies to accept certain capabilities and operational directives. As an example of this authority, Manfra highlighted two examples that supported their directives: the removal of Kaspersky Labs from the federal networks and their directive of agencies to implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to avoid email spoofing. She also discussed the National Cyber Protection System (also known as Einstein) as an extended capability and providing the infrastructure for the National Crime Information Center (NCIC) and partners to perform various analysis like intrusion detection, prevention, assessments, and information sharing.

Robert Perez is the Deputy Commissioner for U.S. Customs and Border Protection (CBP). Perez opened by discussing how CBP in a typical year seizes about 2 million pounds of narcotics, 4,000 fraudulent documents, and 35,000 seizures of violations of intellectual properties valued at over $1.4 billion of OEM retail priced commodities and goods.vHe also shared that CBP is responsible for the economic security of over 390 million travelers, over 26 million containers of cargo, over $2.4 trillion in trade, over $45 million collected duties and fees, and over 100 million cars crossing our borders.

Perez shared an example of a technology application being used by CBP to help them achieve their mission more efficiently. The application is called the Team Awareness Kit, or TAK. TAK is a map-based mobile app that provides real-time shared situational awareness in the palm of an agent's hand through a robust wireless collaboration that enhances the precise location of the agent with the entirety of available resources and technology tools like sensors, targeting tools, and surveillance technologies. So what's the use case? Perez used a possible smuggling operation as a use case for TAK. Rather than using a two-way radio, a border agent can use TAK to immediately share her location and also pinpoint where the threat is. This is critically important when dealing in remote locations where visibility or light may be poor, the topography and geography are challenging, and the vegetation may affect communications.

Figure 1: Gaining an awareness of one's surroundings is a snap with the apps multi-dimensional display. Photo by Jeff Underwood

Patricia Cogswell is the Deputy Administrator for Transportation Security Administration (TSA). In addition to the safety and security of the airports security checkpoints, TSA is responsible for a wide array of other areas like air cargo, over the rail/road cargo, and pipelines. Cogswell shared that this past year, TSA has seen nearly

Jeanette Manfra, CISA, Assistant Secretary

Kathleen Fox, FEMA, Assistant Administrator

Robert Perez, CBP, Deputy Commissioner

Patricia Cogswell, TSA, Deputy Administrator

Key Takeaways:

NPPD has changed their name to Cyber Infrastructure Security Agency (CISA).

ICE and CBP have been very aggressive at moving into the cloud. CBP is over 78% in the cloud today with a goal of 100% eProcessing in the cloud by December 2020.

Datacenter Optimization and Network Optimization are key initiatives for DHS. Specifically, getting data out of the datacenter and network resources into the hands of their agents and field personnel in real-time are critical to their mission success.

Security is essential to

800 million travelers compared to 771 million last year, which poses one of her biggest challenges of moving travelers and packages efficiently through screening checkpoints without sacrificing safety and security. To meet these challenges, Cogswell discussed TSA's commitment to technology investments and industry partnership that help TSA continually adapt and evolve screening technologies, processes, and systems.

As part of this commitment, Casswell discussed TSA's initiative for what she called "Curb to Gate Flow." This is a cross-collaborative DHS initiative with DHS S&T, TSA and CBP that will help travelers navigate airport security and give federal agents a direct line of communication with passengers. This smartphone app would give passengers real-time location information and guide them from curb to gate using Google Maps-style directions. Cogswell shared how much more efficient it would be to receive a notification through the app on your phone from TSA what time and what lane to report to for your checkpoint screening rather than you just waiting in line.

TSA believes this platform will be the basis for a whole segment of smart building applications. DHS's S&T Directorate awarded a nearly $120,000 contract to Locus Labs through DHS's Silicon Valley Innovation Program. Locus Labs is working on a prototype now and will soon launch a pilot program at the Seattle-Tacoma International Airport.

Session II: DHS Security Operations Center Optimization—Crawl Phase

As the result of the 2017 ransomware cryptworm attack "WannaCry" that targeted Windows computers and encrypted user data, DHS security officials decided to consolidate their 17 datacenters spread out over the country to two Enterprise Data Centers (EDCs) known as DataCenter 1 (DC1) located in Mississippi and Datacenter 2 (DC2) in Virginia. This is a multi-year effort so DHS is approaching it from a crawl-walk-run perspective. Paul Beckman (CISO, DHS) moderated the panel discussion which included Alma Cole (CISO, CBP), Kevin Graber (CISO, USSS), Vu Nguyen (Director, Cyber Operations), and Rob Thorne (CISO, ICE) to discuss what "walk" looks like.

Question 1: What are some of the challenges they're facing that made them take a hard look at optimization?

Cyber Operation's Nguyen stated that from an ESOC (Enterprise Security Operations Center) perspective, coordination efforts after hours between the SOC's that are not 24x7 have been a challenge. Nguyen believes optimization will provide more centralized visibility and efficiencies. Today the ESOC focuses on the gateway perimeters like the Trusted Internet Connections (TIC), while the component agencies focus more on the system level. This means there is a process and procedures gap between the ESOC and the components.

their mission success: Security should be "baked" in DevOps applications and not "sprinkled" on later.

DHS's Cloud Factory initiative is a key piece to DHS's cloud efforts. The platform supports the build, test, and deployment aspects of DevOps as well as the operational support to host and secure applications.

EIS will be significant to how they procure cyber and cloud technologies.

Key Technologies:

# DLP

#DevOps

#HVA (High Value Asset) Security

#IAM (Identity and Access Management)

Key Initiatives:

1. Data Center Optimization and Cloud Computing to help DHS move from owning and operating legacy IT, and focus on application management instead of hardware management.

Cole of CBP said, "Threats are not static. Threats continue to evolve as well as our architecture continues to evolve." Since the IT landscape has changed dramatically, DHS needs to change their collective security operations strategies within the department to meet those challenges. Cole is looking at the datacenter optimization initiative to leverage modernization efforts and get data out of the datacenters and into the hands of the agents' mobile devices. To do this, Cole feels CBP will be required to change how they view security, how they interact with data, and how they adopt more cloud and security analytics capabilities.

Kevin Graber, with the US Secret Service feels standardized communication is their biggest challenge because their communication with the ESOC and other components may involve a specific context that may or may not be shared with other components. As a result, Graber is looking at a more risk management/analysis approach to optimization as opposed to just a compliance driven approach.

Question 2: Why do they believe optimization will better position them?

Cole feels optimization will help them better address their shortcomings like policies and procedures, communication, collaboration tools, security automation, and drilling into bi-directional visibility.

Graber stated Hardware Asset Management (HWAM) is useful as a compliance function, but he questions how well they do it. He feels it is crucial to continue to measure their compliance gaps because otherwise it is impossible to improve upon them. Graber shared a real scenario at USSS where he currently has 4-5 people actively tracking down a series of devices to determine their status it over 30 days. On the first of every month, they start the process all over again. They are not taking advantage of their resources efficiently and effectively. Rather than chasing devices, he'd rather have his personnel doing real security tasks.

Question 3: What are some of the technologies and practices industry can use to help DHS?

Cole:

- *DevOps—CBP is embarking on cloud applications which changes the way they code software and building security into the applications.*
- *HVA (High-Value Assets)—currently they have partners doing penetration (pen) testing (min of 1 year now) on all their HVA's but they could use more help with pen testing.*
- *Insider threat and DLP solutions and/or tools are big focus areas.*
- *CBP is looking at standard enterprise logins and standardized reports for enterprise dashboards, so DHS can see what is going on with their systems.*

DHS is championing a vendor-agnostic, hybrid move to cloud. The goal is to have a network where information can flow smoothly across all of their devices and missions.

2. OneNet Optimization approach is aimed at moving to managed services to reduce their technical debt, and position the network to maximize access to the data centers and cloud providers.

3. SOC Consolidation to improve DHS's security posture, secure their data, and provide more centralized visibility and monitoring, The goal is to have a comprehensive display that shows all their devices and see what's on the network across the Department.

Thorne:

- *At ICE insider threat, DLP solutions and/or tools are big focus areas.*
- *Shoring up cloud capabilities from a security perspective is big on his list.*

Nguyen:

- *Cyber Operations wants a solution for a more enhanced supply-chain program.*
- *Insider threat and DLP solutions and/or tools are big focus areas.*

Graber:

- *USSS wants to evolve their ID management and Account Management program; specifically, with (1) mobile device credentials and (2) how they track individuals and track accounts as people's role changes vertically or horizontally.*

Session III: Driving Mission Outcomes Through Information Technology

This session was hosted by Dr. John Zangardi (CIO, DHS) as the moderator with a panel of component CIO's and executives discussing their biggest challenges. The panel consisted of:

- *Michael Brown—CIO, ICE*
- *Dave Epperson—CIO, CISA*
- *Shawn Hughes—Director, EIS PMO*
- *Bill McElhaney—CIO, USCIS*
- *Russell Roberts—CIO, TSA*
- *Donna Roy—Executive Director, Information Sharing and Services Office*

CISA's Epperson is challenged with a lot of legacy systems, so he is looking for breakthrough ideas that will provide him the flexibility of going from their current network environment to virtual machines and micro services quickly and efficiently.

McElhaney is challenged with getting optimization around the network and getting to a place over time to build applications. USCIS is looking at IT solutions that give DHS "velocity" to help respond quickly when the enemy does something. In other words, he would like to get networks optimized around the reality of where they are. McElhaney also discussed how the "Cloud First" policy helped CBP get to around 78% in the cloud today. He feels CBP is no longer in the discovery phase but in a more mature model and looking forward to "Cloud Smart" helping CBP further improve their ability to move to the cloud faster. They are looking to have 100% eProcessing by December 2020.

Brown, of ICE, talked about how DHS' wide area network, OneNet, was novel in 2005, but now DHS's wiring construct needs to change in order to be able to support their cloud initiatives. The most important thing to him is speed, and his customers appreciate being faster over cheaper every time. They are looking at cloud as a means to get capabilities delivered a lot faster.

Roy discussed the status of the “Cloud Factory”, stating that the ATO should be done in December this year. They are building the landing zones for cloud providers so they can comb through the management portfolios. Specifically, they are examining the CXO systems and how to get them out of the datacenter and into a better compute environment. Cloud Factory is a highly automated, secure, reliable set of managed services that provide a set of managed services that allow for a DevOps flow with feedback and innovation for applications. The Cloud Factory platform will ingest user code, assemble the desired machine images (MI), customize the MI configurations, validate security configurations, and deploy the environment in hours as opposed to months. It will also utilize account monitoring tools which will allow the business owner to view usage statistics, costs, utilization data and various dashboards to ensure they are meeting mission objectives.

Other DHS HQ Attendees:

- *Michael Dougherty, Assistant Secretary for Border, Immigration and Trade Policy Office*
- *James McDowell, Asst. Secretary, WMD Office*
- *Ann Van Houten, Executive Director for Oversight, Systems and Support Division*
- *Tom Chaleki, Chief Readiness Support Officer*
- *Nina Ferraro, Acting Deputy Chief Procurement Officer*
- *Kevin Boshears, Director, Office of SDBU*
- *Lesley Field, Acting Administrator for Office of Procurement Policy*
- *Victoria short, Executive Director for Office of Procurement Operations*
- *Jaclyn Smith, Acting Executive Director for Strategic Programs Division*
- *James “Mouse” Neumeister, Deputy Exec Dir., Office of PARM*

Other TSA Attendees:

- *Melissa Conley, Executive Advisor, for Office of Requirements and Analysis*

Other S&T Attendees:

- *Andre Hentz, Acting Deputy Under Secretary*
- *Douglas Maughan, Director, Innovation and Collaboration*