Krystal Covey of DCISE Discusses the DoD-DIB Threat Information Sharing Program with Active Cyber

Posted by: CyberSecurityChief Categories: Spotlight Spotlight - Interviews
No comments

Tools that provide threat information sharing have been a hot technology over the last couple of years. However the tools are only as good as the information that is provided. And the information needs to be timely. And the more context about the threat, the better. And the need for industry outreach and information sharing support about cyber threats has never been greater given the scale and frequency of intellectual property theft and other sensitive military secrets that seem to keep finding their way from our defense industrial base to our adversaries via cyber attacks. All of these "needs" are delivered today by the DCISE program. Led by Ms. Krystal Covey, the DCISE program is in its 11th year of helping the Defense Industrial Base become knowledgeable and alerted to the cyber threat around them. DCISE provides curated threat information from unique government sources as well as from other DIB members. Learn about how this program works in the interview with Ms. Covey below.

Spotlight on Ms. Krystal L. Covey

» Title: Director, Department of Defense (DoD) Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)

» Website: https://dibnet.dod.mil/portal/intranet/

» LinkedIn: linkedin.com/in/krystal-covey-05959992

Read her bio below.

Chris Daly, Active Cyber™: Please explain the mission of DCISE and provide some background on its history as an organization and how it got formed.

Ms. Krystal Covey, Director, Department of Defense (DoD) Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE): In 2008, Deputy Secretary of Defense, Gordon England recognized cyber threats to the **Defense Industrial Base (DIB)** represented an unacceptable risk of compromise to sensitive DoD unclassified information. To "Stop the Bleeding," he directed the DoD CIO to establish a cyber-threat sharing partnership between the Department of Defense (DoD) and the DIB. The **DoD Cyber Crime Center (DC3)** was selected as the operational focal point for the DIB Cybersecurity (DIB CS) program with the DoD-DIB Collaborative Information Sharing Environment (DCISE) established as a subordinate element focused exclusively on interacting with the DIB. The DCISE leveraged other elements within DC3 including the Analytic Group, Technical Solutions Development and the Cyber Forensics Lab. The voluntary DIB CS program initially began as a pilot with 16 companies and has since evolved into a formal DoD program with over 650 DIB participants and their subsidiaries. Originally, the DIB CS participants consisted primarily of major DoD contractors, but today over 50% of the participants are small companies with less than 1,000 employees. Through the DIB CS program, the DCISE shares actionable threat information that informs protection of unclassified DoD data transiting or residing on DIB information systems and networks. When DoD included the requirement to report cyber incidents in DoD contracts, DCISE became the focal point for receiving this information from defense contractors when their controlled unclassified information or personally identifiable information (PII) is impacted.

Active Cyber™: How is DCISE organized to support this mission? What are its key services and functions?

Ms. Covey: DCISE personnel support two areas, the Mission Support Division and the Analytics Division. Mission Support facilitates the interaction with the DIB participants, plans engagements, and oversees process improvement initiatives. The Analytics Division serves as the entry point for receiving and analyzing mandatory incident reporting and voluntary threat information sharing. Analysts produce cyber threat reports that convey time-sensitive security information regarding significant vulnerabilities, malware, intrusion trends, and other cyber threat activity.

Active Cyber™: What other DoD or non-DoD agencies does DCISE rely on for support and why? What other federal/DoD agencies rely on DCISE for help and why?

Ms. Covey: The DoD Cyber Crime Center (DC3) is a Federal Cyber Center and in this role the DCISE capitalizes on a wide range of DoD and U.S. Government agencies for support, including law enforcement and counter-intelligence, the Department of Homeland Security and the Intelligence Community. DC3 leverages whole-of-government capabilities combined with cyber threats and incidents provided by defense contractors to develop both unclassified and classified cyber threat information that is electronically shared with DIB CS participants and U.S. Government stakeholders.

Active Cyber™: What role does DCISE play in managing and enforcing the regulatory requirements involving safeguarding DoD information that resides on DoD contractor networks? How does DCISE engage with DoD contractors in performing this role? What types of mandatory reporting is required by DoD contractors as part of this program? What benefits are delivered to contractors as a result of mandatory reporting in this program?

Ms. Covey: While the focus of the DCISE is primarily on the voluntary sharing program, it does receive and disseminate mandatory cyber incident reports from defense contractors. In support of contractual requirements, the DCISE requests malicious software from companies and facilitates access to compromised media for forensic analysis. This media serves as the basis for cyber incident damage assessments conducted by the Military Departments. **DFARS clause 252.204-7012** mandates that contractors report within 72 hours the discovery of a (likely or confirmed) cyber incident that impacts covered defense information.

Active Cyber™: How does DCISE engage with DoD Industrial Base (DIB) companies to develop participation in the threat sharing program? Is participation voluntary or are all companies that do business with DoD required to participate in the threat information sharing provided by DCISE? What benefits do DoD contractors derive from participation in the threat sharing programs supported by DCISE?

Ms. Covey: Participation in the DIB CS program is voluntary, however only cleared defense contractors are currently eligible to participate (see **32 CFR Part 236**). According to a 2019 DCISE DIB CS Program Partner Survey, the respondents attribute DCISE information as having helped reduce risk for 80% of their organizations and alerted 65% of their organizations to an otherwise unknown threat. The DCISE engages with companies from the executive level to the network defender or Security Operations Center level to encourage sharing of cyber threat information. This information sharing is completely voluntary and company identities are anonymized. DCISE focuses on a customer service approach when engaging a submitter, following up and having a personal dialogue with them to address questions and to develop an understanding of the indicators related to the event. DCISE provides monthly web conferences designed for new participants or new representatives from existing participants, and walks them through how and what to submit and when. DCISE looks for reporting on activity at every stage of the cyber kill chain spectrum. Besides having access to all DCISE threat reporting and analysis services, a DIB CS participant also has access to engagements including Quarterly Working Groups, Technical Exchanges held twice a year in the National Capital Region (NCR), as well as Regional Partner Exchanges (RPEXs) in locations outside of the NCR. The positive interaction and information sharing at these events between Government representatives and other DIB CS participants is a key component of the DIB CS program. A DIB CS participant may also request an Analyst-to-Analyst (A2A) meeting, where information is exchanged at the network defense level, or a Business-to-Business (B2B) meeting where executive leadership from the partner company meet with DCISE executive leadership to understand the value of program participation. Through all of these engagements and interactions, as well as through the online web portal, DIB CS participants achieve a better understanding of the cyber threat landscape and how they can better protect their networks.

Active Cyber™: What techniques, tools, and processes are employed by DCISE to facilitate the sharing of threat information with DIB companies? How are malware artifacts, identified and submitted by DIB companies through the threat sharing program, broken down and analyzed?

Ms. Covey: Unclassified DCISE products are shared with DIB CS participants via a web portal, DIBNet-Unclassified. Classified DCISE products are available to DIB CS participants via a secure web portal, DIBNet-SECRET. The unclassified portal is used by companies to submit cyber incident reports and malware for analysis, and includes forum and chat features for less formal communication. Physical media is submitted via conventional mail services. Once DCISE receives an incident report, malware, or media, it is assigned to an analyst for processing. DCISE's CMMI-SVC v1.3 Maturity Level 3 rating ensures that the defined processes are repeatable and systematically followed. Malware artifacts are typically identified via a company's anti-virus program, log analysis tools, signature-based detection mechanisms, etc. and quarantined for further investigation. These samples are often run through VirusTotal and also submitted to DC3/DCISE for further analysis. DCISE coordinates with and relies upon the DC3 Cyber Forensics Laboratory for in-depth forensic analysis. For a quick turnaround analysis, the DIB CS participant can submit a sample and get results within 20 minutes or less from DC3/DCISE. This analysis gives the submitter some basic information about the sample and can provide details about the malware. For a deeper analysis of submitted samples, DIB CS participants can move the sample to Forensics Laboratory for a full examination that provides a detailed report of the malware sample. DIB CS participants receive all of this support at no cost.

Active Cyber™: What are the types of threat information shared with and by DoD contractors that participate in the threat sharing program? What is the volume of threat information that is shared each year? Does threat data received from DCISE require special handling or is it classified? Does it include signatures that can be easily added to intrusion detection software or to firewalls? How are public cloud environments addressed when it comes to sharing tips, indicators, or incidents?

Ms. Covey: The majority of information shared with DCISE includes incident context, which can provide Tactics, Techniques and Procedures (TTPs); raw indicators, used to identify incidents; and other information that informs our understanding of threats against DIB CS participants. The volume of reporting varies from year to year. All data that DCISE receives from DIB CS participants is considered UNCLASSIFIED//FOUO (For Official Use Only). All voluntary reporting is anonymized to protect the identity of the originator in the analysis process. This preservation of anonymity has served to build a strong trust relationship with the DIB CS participants.

Public cloud environments are addressed like most other public IT systems within DCISE. We closely follow important or critical events, such as potential incidents or breaches of any significant public service, to include cloud environments or managed service providers. As a Federal Cyber Center, DC3 is in a unique position to ensure that any publicly available information or Government Furnished Information is highlighted to DIB CS participants. Any DCISE product may have indicators of compromise and each week, DCISE produces a Weekly Indicator Roundup. A significant number of DIB CS participants automatically ingest indicators of compromise from DCISE products. If a significant breach or cyber incident occurs, DCISE will notify the participants using the DIBNet portal and email.

Active Cyber™: What types of protections are employed for threat or incident data submitted by contractors to DCISE? How is this information used by DCISE and reshared among DIB participants?

Ms. Covey: All DIB participants in the DIB CS program sign a bi-lateral Framework Agreement with the DoD CIO or designee. The Framework Agreement establishes the responsibilities of each party in the program. All DCISE staff and any Government member having access to DIB CS program information must sign a Non-Disclosure Agreement. The DIB CS program respects the confidentiality of all DIB CS participants which is key to creating a strong trust relationship between the DCISE and the DIB CS participants. Information shared by industry partners is anonymized when shared with the rest of the DIB CS participants and the U.S. Government.

Active Cyber™: What are some key operational performance metrics that DCISE tracks to measure mission effectiveness?

Ms. Covey: The voluntary DIB CS program has grown exponentially. Eleven years ago, the program supported 16 companies; DCISE now supports 432, and another 221 wholly owned subsidiary companies, and that number continues to grow. DCISE has published over 9,800 cyber threat information reports, shared over 375,000 **IOC**s, and collaborated with the Forensics Laboratory to perform over 42,000 hours of no-cost forensics and malware analysis for the DIB. The semi-annual Technical Exchanges draw approximately 200 attendees to spend two days discussing and sharing cyber threat information, both unclassified and classified . The Regional Exchanges are often smaller with 20–30 participants, with the most recent event having over 100 participants in attendance.

Active Cyber™: What are the new initiatives being considered or undertaken by DCISE?

Ms. Covey: Over the past ten years, the DCISE has constantly applied lessons learned to continually modify and improve the program. DIB CS participant feedback has been instrumental in providing direction in helping shape the program. DCISE is undertaking several new initiatives to help DIB CS participants address various cybersecurity issues including a new capability to provide assistance to DIB CS participants.

To find out more on this capability and other questions, check out the DIBnet portal at the start of this interview. You can also read more of recent events on the topic of information sharing for DoD **here**.

Thank you Krystal for shedding some light on the DoD-DIB cyber information sharing program. It seems like the program has really taken off under your leadership. I believe the outreach to industry has helped immensely in the fight against cyber attackers, and will likely help even more as information sharing becomes more automated with greater adoption of SOAR technology and threat intelligence tools. I look forward to another status report on the program in a year or so. And thanks to my subscribers and visitors to my site for checking out ActiveCyber.net! Please give us your feedback because we'd love to know some topics you'd like to hear about in the area of active cyber defenses, PQ cryptography, risk assessment and modeling, autonomous security, digital forensics, securing ICS / IIoT and IoT systems, or other security topics. Also, email chrisdaly@activecyber.net if you're interested in interviewing or advertising with us at Active Cyber™.

About Ms. Krystal L. Covey
Ms. Covey is the Director for the Department of Defense (DoD)-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE), located at the DoD Cyber Crime Center (DC3) in Linthicum, MD. DCISE is the DoD designated analysis and reporting center for cyber incidents affecting the Defense Industrial Base. Ms. Covey strives to enhance the security posture and collaborative relationship between DoD, the DIB, and government stakeholders.

Ms. Covey is a cyber intelligence professional with over a decade of experience in this field. She has been with the DCISE for 4 years; and began her tenure as the Chief of Analytics, then assumed the role of Deputy Director. Prior to joining DCISE, Ms. Covey was a Senior Cyber Specialist with the Department of Energy (DOE)-Intelligence (IN), where she assisted in the development of the Cyber Intelligence Unit (CIU) and various product lines. At DC3 Analytical Group (DC3-AG), she led two different teams of Cyber Intelligence Analysts focused on specific nation-state Advanced Persistent Threats (APTs); served as a Federal Bureau of Investigation (FBI) Liaison Officer (LNO) to DC3; was a cyber intelligence analyst for the Department of Justice (DOJ) and began her career as an FBI Honors Intern out of the Baltimore field office.