NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

TOWARD COLLECTIVE DEFENSE:

How DHS Is Helping CISOs and the Private Sector Protect Against Cyberattacks

By Patrick Gaul
Executive Director
NTSC

Toward Collective Defense: How DHS Is Helping CISOs and the Private Sector Protect Against Cyberattacks

In a December 2017 study, the Ponemon Institute noted, “[Most] organizations are only participating in peer-to-peer exchange of threat intelligence (65 percent) instead of a more formal approach such as threat intelligence exchange services or consortium, which contributes to the dissatisfaction with the quality of the threat intelligence obtained.” Yet, more formalized cyber threat intelligence exchange helps increase the security posture of companies, improves security across entire industries, and strengthens national security through public-private partnerships.

Why the lack of participation in more formal programs that include the public sector? Historically, the federal government has only recently begun to develop robust cyber threat intelligence exchanges while ISACs existed for up to two decades (depending on the industry) to fill this need. As DHS has improved its cyber threat intelligence exchange capabilities, it’s struggled against distrust and apathy from the private sector—built up over years of perceptions and habits.

As a result, it’s understandable if CISOs, CIOs, and other security executives view the title of our whitepaper with a similar distrust and apathy. However, we invite the reader to set their skepticism aside as this whitepaper seeks to:

- Review the DHS’s recent evolution and key priorities over the last year.
- Analyze the historical distrust that security executives feel toward DHS, and why.
- Give an overview of what services DHS offers to help CISOs and security teams share cyber threat intelligence—with the goal of protecting companies across all industries and company sizes.
- Show how DHS continues to rapidly evolve, including an overview of several key current and near-term initiatives that will improve its services in 2019.
- Explain why participating with DHS helps strengthen a company’s security posture and improves national security.

DHS’S EVOLUTION IN 2018

Ideally, the Department of Homeland Security (DHS) and the private sector should participate in a bidirectional exchange of threat indicators. However, this exchange currently works mostly unidirectionally—with DHS feeding information to a small percentage of private sector companies. If only a very few companies share threat indicators with DHS, then a potentially powerful program that can strengthen both national security and the security posture of private sector cybersecurity is significantly weakened.

In a CNN opinion article on December 20, 2017, Christopher Krebs, Under Secretary for DHS's National Protection and Programs Directorate (NPPD), said:

"Cybersecurity is a shared responsibility; we all play a part in keeping the internet safe. To prevent another attack like WannaCry, we are calling on all companies to commit to the collective defense of our nation. We must ensure that indicators and information about cyber threats are shared broadly across the community so that more organizations can be inoculated against those threats. All entities—particularly those regularly targeted—benefit when the rest of the population can defend itself. AIS [Automated Indicator Sharing] can be a rallying point for that collective defense, where—with a large enough group participating—organizations of all sizes, regardless of sophistication or investments, work collaboratively to defend our networks and our country."

On August 6, 2018, DHS Secretary Kirstjen Nielsen penned a commentary for *CNBC* urging "collective defense" and more collaboration with the private sector to fend off cyberattacks. According to Nielsen, "[We] aren't 'connecting the dots' quickly enough. Between government and the private sector, we have the data needed to disrupt, prevent and mitigate cyberattacks. But we aren't sharing fast enough or collaborating deeply enough to keep cyberattacks from spreading or to prevent them in the first place."

The concern about improving partnerships between the public and private sector has risen to the level of the White House as seen in its National Cyber Strategy released in September 2018. The White House's strategy acknowledges the private sector's struggles to secure systems at the same time as "adversaries increase the frequency and sophistication of their malicious cyber activities." While critical infrastructure companies are considered the highest priority to protect, the strategy also discusses an overall need for the federal government to "mature our cybersecurity offerings and engagements to better manage […] national risks" and "improve incident reporting and response."

On the heels of the White House, the Department of Defense released an updated version of its cyber strategy—its first update since 2015. Previously operating from a "doctrine of restraint" in cyberspace, the new cyber strategy says the DoD will "defend forward to halt or degrade cyberspace operations targeting the Department" and "preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability." DoD notes that it will provide "public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies"—especially focusing on what DoD terms "defense critical infrastructure" and "defense industrial base" companies.

Despite legitimate concerns from CISOs and the private sector about the still young AIS program from DHS, the recent language from the White House, DoD, and DHS shows that the stakes of participation in such a program are much higher today than they were even two years ago. The day-to-day worries of CISOs have become more intertwined with national security. However, it's understandable to show skepticism when "collective defense"—a concept used by entities such as NATO—is used to describe the relationship between DHS and the private sector. Is this simply hyperbole from DHS—a desperate attempt to get CISOs to participate in a program under scrutiny from Congress and under pressure to show results?

Trends this year show that it's not hyperbole. Before examining some important aspects of AIS, the Cyber Information Sharing and Collaboration Program (CISCP), and Enhanced Cybersecurity Services (ECS) that may currently benefit (and even surprise) CISOs, let's first look at a bit of history and context that shows how much the cybersecurity landscape has changed since AIS's inception in 2015.

Lines blur more often between national security and private sector cybersecurity.

In the early days of the internet, many cybersecurity issues were mostly expensive annoyances but not national security threats. When dealing with a threat, it was clearer when to involve the military or law enforcement—or when to just let the private sector take care of themselves.

Today, what is WannaCry? A business disruption? A criminal act? An attack by North Korea on the United States? All the above? Some of the above? More than a year later, we're still analyzing how the United States should have best responded to this incident.

Since WannaCry, we now see daily headlines about these blurred boundaries such as Russia attacking United States election systems and critical infrastructure. According to the 2018 CrowdStrike® Global Threat Report, "The distinctions between state-sponsored actors and cybercriminals are becoming blurred, as nation-state adversaries adopt eCrime TTPs such as ransomware, and criminal groups perpetrate more sophisticated targeted intrusion-type attacks." Pinning down culprits also becomes more problematic as nation states publicly hide behind "rogue" cybercriminals.

CISOs feel more and more at a disadvantage fighting asymmetrical attacks.

Some cyber attackers operate with an unfair advantage against companies. A nation state, for example, may have significantly more sophisticated resources that allow them to breach a company's security without detection. Even if cyber attackers are less sophisticated than a nation state, they often know that one chink in a company's security armor is all it takes to carry out a breach. These situations are asymmetrical—meaning that a cyber attacker's unfair advantage increases the probability of a data breach becoming successful.

Because of traditionally clear legal boundaries between how the military and law enforcement can respond to an attack versus how the private sector can respond, CISOs have struggled more recently to fend off such cyberattacks. While they can strengthen cybersecurity and make incremental improvements, a private company can't retaliate against a nation state or take down a sophisticated group of organized cybercriminals operating in different countries.

This asymmetry and a historical lack of US government assistance with cyberattacks has led to:

- The creation of ISACs to help specific industries protect themselves.
- The emerging and now prevalent role of the CISO to bring cybersecurity more prominently into focus in the boardroom.
- Inspired recent bills such as the Active Cyber Defense Certainty Act (ACDC) introduced by Representative Tom Graves (R-Ga.) and the Cyber Deterrence and Response Act of 2018 introduced by Representative Ted Yoho (R-Fla.) (passed by the House in September 2018).

Unfortunately, many companies feel that they are thrown to the wolves after a cyberattack or major data breach—as seen by negative media coverage, lawsuits, and government investigations that emerge in the wake of an attack. Rather than encouraging the sharing of cyber threat information, this hostile environment causes companies to retreat and retract—keeping data close to their chest.

A history of distrust exists between the public and private sector over cybersecurity.

After many years of private sector frustration with DHS and other federal agencies concerning information sharing, Congress passed the 2015 Cybersecurity Information Sharing Act, which "[required] the Director of National Intelligence and the Departments of Homeland Security (DHS), Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats." It mandated that DHS "receive indicators and defensive measures that are shared by any entity" and "ensure that appropriate federal entities receive shared indicators in an automated, real-time manner" while also providing liability protections for companies.

As a still relatively new law, its implementation and the evolution of its mandates arrived after years of historical distrust between the public and private sector. To be fair, these agencies are relatively new in our nation's history and often figuring out roles, responsibilities, and programs on the fly (which is admirable within the context of a slow-moving government). In addition, cybersecurity is an unprecedented challenge for all organizations—not just the federal government. When national security, law enforcement, and legal nuances become involved, federal agencies need to tread carefully—and slowly.

Even keeping this in mind, we have heard CISOs at dozens of NTSC events over the past two years often espouse a litany of frustrations that have included:

- A lack of detailed updates about how DHS's information sharing works, what it's doing, and what progress it has made.
- A lack of transparency about the VEP (Vulnerabilities Equities Process).
- A feeling that DHS doesn't share important information about nation state and international criminal attacks—and does little when these threat actors are identified.
- A lack of feedback about the value of information that private sector companies share with DHS.
- Concerns about the quality of DHS information shared with the private sector such as stale, unscrubbed, or non-contextual data.
- Security issues around the information collected by DHS (especially in the wake of significant federal government data breaches).
- Issues related to federal cybersecurity staffing and bandwidth—especially with security clearance backlogs, an inability to pay for top cybersecurity talent, and bureaucracy.
- Declassification issues as even companies that want to participate in public-private information sharing can't participate because they literally are not allowed to view shared threat indicators.

The good news is that DHS steadily makes progress tackling these issues, whether real or perceived. However, when progress is slower than CISOs prefer, they are more likely to prefer relying on ISACs or other cyber platforms—skipping DHS entirely. That's why the NTSC's mission to promote dialogue, education, and government relations between the public and private sector is so important in this context.

A FRESH LOOK AT AUTOMATED INDICATOR SHARING (AIS)

At the NTSC's Northeast Regional CISO Policy Roundtable in February 2018 and the NTSC National CISO Policy Conference in July 2018, DHS Deputy Assistant Secretary Rick Driggers outlined the services DHS provides to the private sector including automated indicator sharing, incident response, and critical infrastructure vulnerability assessments. He also shared some insights about the latest processes and mechanisms of DHS's AIS information sharing program.

Setting aside past differences and opening themselves up to dialogue, CISOs had many questions for Driggers about incident response processes, delays obtaining security clearances, and the overall role of DHS. This fruitful dialogue highlighted the importance of such public-private sector interaction and showed that a more productive, positive path forward exists.

For CISOs, it's worth a review to examine current DHS programs and the services they provide. Then, we'll look at some developments that may soon alleviate many of the lingering, historical information sharing issues between DHS and the private sector.

Automated Indicator Sharing (AIS)

While DHS "boasts" about 250 entities (including companies, ISACs, and government agencies) participating in AIS as of July 2018, it's clear that's not a large number—and DHS is aware of the low numbers. However, the organizations already participating (especially ISACs and government agencies) already provide a lot of useful information. Government networks—which were estimated in 2017 to include 20 percent of the total networks in the United States—all participate. Plus, information from DHS is distributed to many partners of the estimated 250 entities, reaching even more organizations. The information collected and shared is currently more robust than it first appears.

While DHS offers plenty of information about AIS on its website, a few points are of particular interest to CISOs:

- **No cost to participate in AIS**: Unlike some services that federal agencies offer, the AIS program is free—although indirect costs such as attorney fees, required equipment, and staff time may still be pricy depending on company size.
- **Automated threat indicator sharing in real-time:** As DHS collects information about threat indicators (such as malicious IP addresses, phishing email sender addresses, domain names, etc.) through its own research or shared by its members, it shares that information in real time. This sharing is especially useful when zero-day vulnerabilities or other fast-moving threats are occurring. Here, DHS emphasizes "velocity and volume" over validation—which can also lead to issues about context.
- **Liability protection**: The Cybersecurity Act of 2015 "grants liability protection and other protections to companies that share indicators through AIS."
- **Data privacy protections**: DHS notes that it "has taken careful measures to ensure appropriate privacy and civil liberties protections are fully implemented in AIS and are regularly tested."

Incident Reporting and Response Teams

Many CISOs did not realize DHS provided a variety of incident response services that it will deploy, if needed and appropriate, to any large company. **NCCIC** (formerly **US-CERT and ICS-CERT)** "develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners." Information security teams can report cybersecurity incidents through the NCCIC / US-CERT website, and AIS will analyze and respond to the incidents. DHS considers this "asset response" and takes lead on it (while the FBI takes lead on "threat response").

According to a DHS fact sheet, "Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community." CISA / NCCIC also offers onsite incident response services for critical infrastructure organizations in addition to information sharing and analysis. Specifically, "Cybersecurity and infrastructure protection experts from CISA / NCCIC provide assistance to owners and operators of critical systems by responding to incidents and helping restore services in both business and control system environments."

Vulnerability Scanning and Assessments

Through AIS and the National Cybersecurity and Communications Integration Center (NCCIC), National Cybersecurity Assessments and Technical Services (NCATS) can provide vulnerability scanning, phishing campaign assessments, risk/vulnerability assessments, and validated architecture design reviews. The NCCIC also offers malware analysis and vulnerability coordination that includes an Advanced Malware Analysis Center, Advanced Analytical Laboratory (AAL), and Vulnerability Coordination.

Cyber Information Sharing and Collaboration Program (CISCP)

Relying heavily on analyst-to-analyst information sharing, DHS's Cyber Information Sharing and Collaboration Program (CISCP) "enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors." With CISCP, private sector companies get more heavily involved with DHS but also receive more in return.

- **Curated bulletins, alerts, and other content**: DHS sends out curated, contextually-aware information such as summaries of current threat activity ("most frequent, high-impact types of security incidents"), alerts ("timely information – current security issues, exploits, vulnerabilities"), indicator bulletins ("new vulnerabilities and patches"), analysis reports, priority alerts, tips, and recommended practices. Some tips and best practices are delivered non-technically so that business owners can understand important cybersecurity issues. ICS-CERT also creates specialized content for critical infrastructure entities.
- **Monthly and quarterly analyst briefings, exchanges, and events**: These briefings dig deeper into patterns, major issues, and proactive ways to fend off cyberattacks. Because they are informed by DHS intelligence and information collection, these briefings have a lot of value.
- **Security clearances and access to the NCCIC watch floor:** Members of your company can literally stand on the ground floor of DHS's information collecting and sharing center while also accessing classified information.

Enhanced Cybersecurity Services (ECS)

DHS offers a service to supplement an organization's existing information security that "follows a managed security service model whereby DHS shares sensitive and classified cyber threat information with accredited ECS commercial service providers. These commercial service providers in turn use that information to detect and block malicious traffic from entering or exiting customer networks depending on the service." DHS says that ECS is "the only cybersecurity capability on the commercial market that uses sensitive and classified cyber threat information to protect networks" and "the only way you can operationalize classified information to immediately protect your network."

ISAOs

For organizations that can't join an ISAC but need cyber threat information similar to an ISAC, DHS provides ISAOs. The University of Texas at San Antonio coordinates the creation of voluntary standards and guidelines for these companies. According to DHS, "Through public, open-ended engagements, the ISAO Standards Organization will develop transparent best practices that align with the needs of all industry groups, not just those traditionally represented by ISACs."

WAYS THE AIS IS ELIMINATING PAST PROBLEMS AND BECOMING MORE VALUABLE

While all these services are currently valuable, they are also continuing to evolve into more valuable—and important—programs for both private sector companies and national security. DHS clearly desires to change the existing paradigm on its communication which, in the past, has not been rated highly by the private sector (and which DHS acknowledges). Going forward, DHS is taking steps toward creating productive dialogues that help everyone to participate and benefit from its programs.

In a November 2017 DHS report, the agency outlined three specific areas of needed improvement for its AIS program:

- "Emphasis needed on sharing quality cyber threat indicators and defensive measures"
- "Cross-domain solution and automated tools could promote timely sharing and analysis of cyber threat information"
- "Enhanced outreach could increase participation and usefulness of the AIS program"

DHS has worked to address the quality and timely sharing of threat indicators by moving to STIX [Structured Threat Information eXpression] 2.1 and TAXII [Trusted Automated eXchange of Indicator Information] 2.x in 2018. The STIX improvements are specifically being implemented to improve the speed and context of information sharing.

In a *Federal News Radio* article, John Felker, the director of the NCCIC at DHS, said, "Part of the problem with the formatting is we had to go through a lot of testing to make sure the data that is going out is valid and it's not going to create a whole lot of false positives. In each case, we do that with some rigor for each of the partners. With a couple of the big companies that we are playing with now, that already has been accomplished and we continue to improve that process."

In April 2018, an article in *Inside Cybersecurity* noted that "The Department of Homeland Security is testing a new system over the next few months to improve the quality of its information and threat-indicator sharing program, which will involve input from five or six multinational corporations to bolster its analysis, according to a senior DHS official." This new system is focused on the quality of information that DHS shares, and DHS invited a few multinational private sector partners for help in testing this new system.

By making these improvements, DHS is directly addressing issues of trust and threat indicator information quality. In July 2018, Driggers acknowledged at the NTSC National CISO Policy Conference that DHS had received lots of feedback to help improve AIS as they planned to update to AIS 2.0 and STIX 2.1. These updates will allow DHS further opportunities for upgrades and improvements to how AIS works. DHS is aiming for feedback at machine speed, more relevant indicators with more context, and better confidence metrics.

These technical improvements are important because information sharing is at the heart of DHS's overall cybersecurity strategy released in May 2018, especially when considering the department's goals of:

- Assessing evolving cybersecurity risks
- Protecting federal government information systems
- Protecting critical infrastructure
- Preventing and disrupting the criminal use of cyberspace
- Responding effectively to cyber incidents
- Strengthening the security and reliability of the cyber ecosystem
- Improving the management of DHS cybersecurity activities

When discussing the protection of critical infrastructure, DHS says in its strategy document that it "must deepen technical collaboration across all the sectors and with other key nonfederal entities on risk mitigation efforts." The strategy later points out that "DHS must also implement mechanisms to ensure that asset and threat responders, informed by the intelligence community, share information with each other, with sector specific agencies, and with the private sector to inform all related incident response efforts."

DHS also announced on July 31, 2018 the creation of the National Risk Management Center. According to DHS, the National Risk Management Center will create a crosscutting risk management approach between the private sector and government to improve the defense of our nation's critical infrastructure. It aims to be "a single point of access where government and the private sector can collaborate across sectors to develop plans and solutions for reducing cyber and other systemic risks to national and economic security."

As an example of how this new center can serve the private sector, DHS created the Information and Communications Technology (ICT) Supply Chain Task Force to "examine and develop consensus recommendations for action to address key strategic challenges to identifying and managing risk associated with the global ICT supply chain and related third-party risk. The Task Force is intended to focus on potential near- and long-term solutions to manage strategic risks through policy initiatives and opportunities for innovative public-private partnership." It put out an RFI on July 31, 2018 requesting feedback by October 11, 2018.

In October, the NTSC applauded the passage of the Cybersecurity and Infrastructure Security Agency Act by the US Senate. This bill redesignates the NPPD as the Cybersecurity and Infrastructure Security Agency (CISA). By rebranding the NPPD and elevating it to the status of a standalone agency under DHS (giving it the same status as the Secret Service and the Transportation Security Agency), this bill helps the United States better protect critical infrastructure and strengthen public-private sector partnerships around cybersecurity. The legislation reflects the needs of the private sector to work more productively with DHS to share cyber threat intelligence and communicate about critical cybersecurity issues that affect national security. A dedicated agency such as the CISA, with a clear mission, helps DHS carry out this important work.

TOWARD COLLECTIVE DEFENSE: SOME CONCLUDING THOUGHTS

Even if CISOs feel that federal information sharing may not be improving as fast as they'd like, there are clear reasons to reconsider engaging with DHS:

- **DHS is aware of its limitations and specifically addressing these shortcomings**: This isn't just talk. DHS is backing up its realizations with reports, specific areas needing improvement, and tangible steps forward. This activity suggests that AIS will evolve like other government agencies in the past—starting off a bit wobbly but eventually becoming a critical partner with the private sector.
- **DHS and the private sector need to partner because cybersecurity threats are more often becoming national security threats**: Because the lines are now so blurred between nation state attacks and private sector cyberattacks, partnering with an organization like DHS can be more impactful than going it

alone or just sticking with ISACs. DHS and other national security agencies can respond and retaliate in ways that the private sector—even with ISACs—cannot.

- **Partnering with DHS now means influencing the department's future direction**: As Driggers showed at our recent roundtable, DHS is looking for partnerships, input, and ideas. CISOs participating now will have a willing ear from DHS—especially through the briefings and contacts made through participation in the agency's programs.

As DHS addresses these problems and more companies participate, AIS will become more useful and important for not only CISOs but also for national security. The NTSC has already established a dialogue with DHS and wants this dialogue to be ongoing. An organization like the NTSC can be of assistance in helping DHS with these kinds of efforts—bridging the gap between the needs of the private sector with the current and future capabilities of DHS. To date, we have relayed feedback from CISOs to DHS about its problems and invited speakers such as Driggers to directly engage with our members and event attendees.

To help with DHS's efforts, **we encourage CISOs and their suppliers to sign up for AIS, CISCP, and any other programs that make sense.** This participation will help build information sharing trust between the public and private sector that has eroded over time while also helping us look forward as a nation in building a true collective defense where all parties work together to increase the nation's security posture and overall national security.

*If you would like to learn more about how these DHS programs can help your organization, please contact the National Technology Security Coalition at **patrick@ntsc.org or 404.920.0703.***

*You may also contact DHS at **www.us-cert.gov/ais** or **ncciccustomerservice@hq.dhs.gov** for additional information and to join AIS.*

Patrick D. Gaul is the Executive Director of the National Technology Security Coalition (NTSC), a non-profit, non-partisan organization focused on uniting both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness. An industry leader and subject matter expert in technology products and services, Patrick has held many senior positions in sales, marketing, and channel management.

NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION