Observations, Insights, and Lessons Learned from Cohort 2021

U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Idaho National Laboratory

Introduction

The Operational Technology (OT) Defender Fellowship is a highly selective education program for middle- and senior-level OT security and operations managers across the U.S. Energy Sector. The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) created this program to provide participants unique opportunities to build relationships with their industry peers and with cyber experts in U.S. government departments and agencies. Participants gain a greater understanding of the OT threat landscape and strengthen their capabilities to defend critical energy infrastructure. OT Defender Fellowship (OTDF) participants meet four times during the year-long program.

The feedback from the first cohort of the OTDF was positive. The program is making a meaningful difference for both the participants and the Energy Sector as a whole. Members of the 2021 cohort were eager to share what they learned within their organizations, noting the program has brought value to their companies and positive attention to the importance of OT security. They see the value gained from participating in the OTDF and want their peers to benefit from the same opportunity. In the wake of the final session of the first cohort, one of the Fellows briefed his peers as part of a subsector cybersecurity task force meeting. He noted, "At least half of the persons in attendance wanted to put their name/organization in the running," to participate in future years.

The Fellows noted that throughout the program, the U.S. government's desire for cooperation with industry came through loud and clear. The Fellows and their employers likewise want a constructive, bi-directional relationship with government leaders and offered feedback on ways to continue to build and improve public-private collaboration in general. The following report outlines the positive ways the program is impacting public-private collaboration and offers areas for improvement and ways to build upon successes for future cohorts.

OTDF Enhances Public-Private Collaboration

Despite COVID-19-driven restrictions requiring some virtual sessions and schedule flexibility, Fellows commended the robust relationship-building aspects of the Fellowship. One Fellow applauded the Fellowship programming, noting, "We were able to talk to experts across multiple agencies, all the way to the bottom. No one within the business has had that breadth of exposure." Another said, "This program builds bridges and gets OT Defenders in front of policy makers in the ways other programs have not."

Fellows have already begun leveraging the program to create complementary relationships with experts at Idaho National Laboratory (INL), as well as departments and agencies throughout the program. As a result of the Fellowship, participants have engaged with other CESER programs such as Cybersecurity for the Operational Technology Environment (CyOTE) and are eager to participate in new public-private programs. Program staff is fielding requests for additional introductions, continuing to play this role now that 2021 Fellows have transitioned to program alumni.

Proactive Engagement: Fellows were particularly interested in engaging with the U.S. government to proactively share information, rather than just reaching out to agencies for assistance following a cyber incident. Fellows noted that personalized engagement between individuals in industry and government helps build the kind of trust necessary for effective information sharing, crediting the Fellowship with helping facilitate this. One Fellow noted the strength of the relationship his company was building with the local Federal Bureau of Investigation (FBI) office. "Our company would not be working as closely with the FBI as we are right now if it wasn't for the OT Defender Fellowship," he said. Throughout Cohort 2021, the FBI stressed that a primary goal of their engagement is to strengthen or, where needed, establish the relationship between the Fellows and the cyber experts in the relevant Field Office. The Fellowship is beginning to deliver on this goal.

Cohort 2021 coincided with President Biden's Industrial Control Systems (ICS) Cybersecurity Initiative. The initiative started with the Electricity Subsector's 100-Day Action Plan and next expanded to the Oil and Natural Gas Subsector. Throughout the program, the Fellowship held roundtable discussions about the initiative and reflected on successes and challenges. Fellows commended the program's focus on ICS security and noted the Administration's attention to the topic led to a similar increased focus by company leadership. However, Fellows also expressed concern that consistent reference to the larger activity as "100-day plans" provides a misleading impression (particularly amongst audiences without as much relevant context, such as mainstream media and the general public) that efforts would be substantively completed, and risks mitigated by the end of the sprint. Instead, the effort is continually evolving, requiring persistence to improve resilience and apply mitigation efforts.

Fellows expressed the desire to proactively participate in programs such as the ICS Cybersecurity Initiative and 100-day action plans. They also provided constructive criticism around the concern about practical data sharing and interoperability. For example, Fellows worried that despite high-level assurances, sensor vendor selection and technical implementation details may make it challenging for companies that have purchased a competitor's product to be able to fully participate.

Ongoing feedback loop: There was consensus across the group about the desire for consistent and sustained engagement with the U.S. government. The Fellows discussed the value they could provide, representing a broad cross-section of the Energy Sector with diverse perspectives and experiences. As such, the Fellows believe they could offer a valuable forum where government could receive feedback and input on policies, decisions, and issues affecting the critical energy infrastructure. The Fellows recommend DOE and its

agency partners use current Fellows and the Fellowship's growing alumni network as a sounding board to receive direct, 'in-the-weeds' feedback without the requirement of a conversation driving toward consensus.

Resources available to industry: Briefings with departments and agencies provided a greater understanding of the breadth of valuable programs, resources, and trainings available to asset-owners of critical energy infrastructure and other critical infrastructures. One Fellow commented, "This program provides a great overview of all of the programs available to critical infrastructure." The Fellows encouraged OTDF program staff and interagency partners to make this even more seamless by incorporating "how to apply / join / participate" at the end of each briefing along with a frank assessment of what participants can expect to gain and what they will be required to do. They also reflected it can be challenging for security managers to ensure their companies are taking full advantage of the ever evolving and expanding opportunities. There is a fear that companies are missing out on timely opportunities because they do not know what resources are available. The Fellows are seeking consolidated lists of resources such as the "U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) Services Catalogue,"[a] and encouraged the DOE to put together a similar product that offers a "one-stop-shop" listing of all programs and resources. The Fellows want one list of all programs across the entire U.S. government but recognize each department and agency is likely best equipped to create only its own program offering list.

Peer-to-peer sharing: During the program, Fellows not only learned from government experts but also from their peers. Fellows learned about everything from how to address threats to how to communicate the importance of OT security to executives. The Fellows shared best practices on supply chain and vendor security, the deployment of cybersecurity tools in OT environments, and incident response. They also volunteered to lead discussions among themselves to share lessons learned—an idea the program staff is implementing in follow-on cohorts. They applauded the collaborative environment of the program, with one Fellow commenting, "The deep thinking and safe group space create a good environment for leaders to talk, and the more experienced to help the less experienced."

The program staff was also heartened to learn the Fellows went to dinner together nearly every night during Sessions 3 and 4, sharing stories and experiences. Spontaneous discussions in informal settings are a desirable outcome, where the Fellows can build trust and share information authentically and organically. During Cohort 2021, Session 3 was the first in-person session because of COVID-19, and thus some of the interpersonal relationship building occurred late in the year. That said, the Fellows all emphasized the importance of relationship building and maintenance aspect of the Fellowship. For future cohorts, the program staff is continuing to encourage this informal relationship building.

[a] https://www.cisa.gov/publication/cisa-services-catalog

Areas for Continued Growth

Single entry point into the U.S. government: Critical energy infrastructure asset-owners want a single-entry point to access all relevant U.S. government departments and agencies. During an incident, a company has fixed resources (time and personnel) to make notifications and respond to inquiries to ensure every external organization has received the information it requires or requests. Asset-owners want to be able to make "one phone call" and know the information will be shared with other relevant government agencies. This is as true in non-crisis situations as it is during incidents. Asset-owners want to be able to voluntarily provide information—once and in a single format—and have the confidence this information is dispersed to all necessary recipients. The Fellows expressed frustration with previous interactions with government partners (both during cyber incidents and during proactive information sharing) when multiple agencies would ask for the same information from the company rather than sharing it with each other.

During engagements with departments and agencies, Fellows consistently asked, "If I have an incident, who should I call first?" Government respondents predictably explained why contacting their own agency was the best first step. This was particularly, although not uniquely, prevalent during conversations with FBI and CISA representatives. Fellows also recognized the unique role the DOE as the Sector Risk Management Agency (SRMA) can play as the government lead during a crisis response because of its unique knowledge and long-term relationship with companies. One Fellow noted the impact the Fellowship had on his company's incident response plans, saying, "The discussions with my peers about their interactions with agencies during an incident have led me to refine and modify my incident response plans." Another Fellow noted the importance of coordination and collaboration between sector risk management agencies, particularly as it relates to subsectors that may interact with another SRMA in addition to, or instead of, DOE. This collaboration is also important where two or more critical infrastructures meet.

During a roundtable discussion, the Fellows articulated their desired end state is a "Cyber 911 dispatch" in which critical infrastructure asset-owners call a single office that is able to quickly identify those available federal, state, and local resources that are ready to assist. While the FBI is likely to assert CyWatch serves this purpose, the Fellows articulated that in their experience, in practice CyWatch does not (currently) have the necessary visibility into the supporting resources at other federal agencies, let alone state and local resources.

Expectations of Industry / Government Capabilities: The Fellows felt the government at times has unrealistic expectations of the capabilities and knowledge of industry. This manifests in different ways. There is often an assumption large companies have significant capabilities and resources and could make greater cybersecurity investments more easily than their smaller counterparts. There is also an assumption that if industry would provide all its data to government, the findings would be self-evident. Broadly speaking, asset-owners do not purposefully withhold information that could provide government analysts the

"missing link." The Fellows also noted a perceived assumption that particular individuals in a given conversation have or can easily gather broad and deep knowledge across their entire organization, as opposed to having expertise in certain areas and less familiarity elsewhere. In fairness, this phenomenon is not unique to government officials; it is common across most individual-on-behalf-of-organization interactions. During conversations about the Transportation Security Agency's (TSA) security directives for pipelines, for example, Fellows expressed frustration with requests for bulk data submissions as well as a requirement for companies to provide a single point of contact to the U.S. government, which are requests askew with good resilience practices.

Similarly, there appears to be a disconnect across both government and industry between the perceived responsibilities and the practical capabilities of securing the supply chain. Echoing broad public concerns and the government's own focus on the issue, supply chain security was a frequent topic of conversation within the Fellowship. Some of the first conversations and information exchanges between the Fellows were comparisons of experiences with vendors and products in the context of major investment decisions. Asset-owners recognize the significant security risk they are assuming with less than adequate transparency into the digital products critical to their operations. However, the scale and complexity of this risk is greater than any single organization can effectively mitigate. Asset-owners are significantly limited in their practical ability to hold suppliers accountable for security performance; simply buying or not buying a product from a particular vendor may not influence that vendor's security practices.

The Fellows were encouraged by briefings about DOE's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program for its ability to provide some useful information, but some have overly ambitious expectations of the program's ability to quickly scale and its efficacy of a possible future approved list of products and vendors. Ultimately, the Fellows recognized neither the U.S. government nor industry alone has the capabilities to solve this challenge. With challenges of this scale and complexity, the Fellows argued public-private collaboration is essential. They also noted more broadly, sustained, regular interactions between government and industry representatives will help both parties more fully appreciate the capacities and limitations of the other; all while assuming sincere intent.

In short, both industry and government seem to believe the other has extraordinary insights or unique capabilities they are unable or unwilling to share. This mismatch is the result of siloed organizations that do not have interpersonal trust relationships with each other. Neither side can see the whole of what the other knows and has no way to confirm accuracy and/or authenticity. The Fellowship aims to remedy this situation by building interpersonal trust and relationships between individuals in industry and government. Rather than interactions between faceless entities, the Fellowship builds relationships between individuals. These individual trust relationships are the foundation from which a successful public-private partnership wholesomely exploits transitive trust to improve security and reduce risk to the collective. The Fellowship aims to help participants understand the roles and responsibilities of government so Fellows recognize how they can be indirect

beneficiaries of government activities, even when they are not privy to the inherently governmental details.

Frustration with messaging and legal authorities: Program staff also observed the Fellows' frustration regarding the limitations on authorities that prevent direct engagement between asset-owners and certain agencies, particularly those in the U.S. intelligence community and the U.S. Department of Defense. The Fellows appeared frustrated by the conflicting messages from the Administration, Congress, media, and public that energy is a uniquely important critical infrastructure sector; and yet legal restrictions prevent components of the U.S. government from directly engaging with critical energy infrastructure owners and operators. This frustration is tied to the friction regarding classified briefs and mismatched expectations. Industry cannot see how government capabilities benefit them because interagency information sharing (even more so within the intelligence community) is opaque, compartmentalized, and tightly controlled. Instead, Fellows experience the cognitive dissonance of agencies declining to engage meaningfully with them, despite the message of the criticality of their sector.

That said, during the Fellowship, participants gained a better appreciation for why they are more likely to directly receive information from some agencies (such as DOE, DHS CISA, and FBI) rather than others (such as the National Security Agency [NSA]). The Fellows were heartened and encouraged by more multi-sealed products, cross-branding, and cross-referencing of alerts so the recipients can quickly recognize if the information is new or repetitive; thereby making the ingestion of information and responses efficient. It can be challenging for companies to ensure they are accurately ingesting all relevant security information and products. Fellows explained they often receive similar or identical information packaged differently from government and private agencies. This overlapping information is generated by information sharing and analysis centers (ISACs), sector coordinating councils, InfraGard, commercial providers, and other resources. While this can be helpful for assured transmission and amplification, it is not always clear if additional emphasis is intended, or if the information is merely duplication or the product of circular reporting.

Program Curriculum: As the first cohort of the OTDF, the participants recognized they were paving the way for future programs. Participants requested additional content throughout the Fellowship. For example, in response to interest in better understanding the role of federal law enforcement in administration strategy, program staff recruited the Assistant Attorney General for National Security to brief the group. When Fellows asked for more insight into policymaking, program staff recruited Sen. Angus King (I-ME) to speak to the group. These components have been incorporated into future curricula.

The Fellows also offered constructive criticism, to which program staff have attempted to be very responsive. Cohort 2021 noted they hoped for more and deeper technical discourse. They were interested in learning from U.S. government partners and industry peers about technical and sector-specific cybersecurity best practices (beyond cyber hygiene), as well as ways other organizations had addressed the challenges they are struggling to tackle. The

program staff began implementing this feedback during Session 4, continuing into the curriculum for Cohort 2022. This includes hosting the capstone experience (Session 4) at an alumni facility where Fellows could go onsite to engage in technical discussions with alumni of the program.

Fellows also agreed that more focus on "left-of-boom" content would improve the Fellowship curriculum. Also related to a desire for more technical content, Fellows said during Session 3 they would have benefitted from discussions about how companies are designing their systems and testing / evaluating response plans and procedures in advance of an incident. These types of proactive planning and scenario-based assessment can allow Fellows to test their own assumptions about design and preparation built into the capstone experience. Program staff provided this feedback to agency partners for Cohort 2022, planning to emphasize to briefers (and the offices they represent) the industry's desire for proactive engagement.

Obtaining security clearances for Fellows who were not already cleared was a long process. Even after all Fellows were cleared, other challenges emerged. Agencies often did not have the staff or facilities for classified briefs, asserting the incremental value over an Official Use Only (OUO) discussion was not worth the logistical effort; noting all conversation could remain at an unclassified level. Despite these challenges, program staff have decided not to require OTDF applicants to have a security clearance prior to selection as this could limit highly qualified candidates who would both provide value to and benefit from the Fellowship.

Cohort 2021 had its first classified discussion during Session 4, and members praised the exchange. They appreciated the briefer's candor and unique ability to contextualize the information. Given the value of this session and the potential benefits from other classified or 'closed-door sessions,' the Fellowship will continue to prioritize the inclusion of such discussions despite the challenges.

Setting aside the logistical challenges, the program staff witnessed a mismatch of expectations around classified briefs. There is a common assumption that the government possesses information that, once shared, could materially change the security risk calculus and behavior of individual companies. The Fellows recognized this is a simplistic and not wholly accurate assumption, challenging government briefers to do a better job communicating in an unclassified setting. The Fellows also recognized information provided in classified settings can be difficult to act upon. Tear lines should become the norm as a "take-home" product. It should be noted classified discussions do have value. Asset-owners do not always appreciate the underpinnings of public or OUO reports and alerts, and classified briefings improve industry confidence in the unclassified products. Having received a classified brief, Fellows may still be unsatisfied with the content because briefers have specific constraints around what can be conveyed and often cannot answer follow-up questions at the same security clearance level as the prepared briefing. Rather, two-way discussions held in a classified setting are likely to be more illuminating and offer greater opportunity for useful information exchange.

Conclusion

The positive responses received from the Fellows confirmed DOE's assessment of the need for the OTDF. Feedback from the Fellows will continue to help program staff develop the curriculum and craft an effective, enriching experience for future cohorts.

The Fellows also expressed a desire to remain engaged with the program as alumni, including collaboration with future cohorts. Program staff is exploring how to transition ad hoc opportunities such as invitations to existing briefings into a more fulsome program for alumni.