Operational Technology Defender Fellowship™

Observations, Insights, and Lessons Learned from Cohort 2023

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

INL Idaho National Laboratory

Introduction

The U.S. Department of Energy's Operational Technology Defender Fellowship (OTDF) continues to provide middle- and senior-level OT security and operations managers unique opportunities to engage with federal agencies and develop the relationships essential for enhancing the cyber resilience of critical energy infrastructure. Created by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) in 2020 and launched in 2021, the year-long fellowship includes four in-person, week-long sessions and multiple virtual intersessions during which Fellows gain a greater understanding of the roles, responsibilities, and capabilities of various government agencies including how they themselves might work with these agencies to enhance their organization's security or respond to a cyber incident. As one Fellow noted, "I have a much clearer understanding of how the various Agencies work to help secure critical infrastructure."

The 2023 Cohort was the third to complete the program. As such, the curriculum has solidified – even as program staff continue to work with partner agencies to make slight adjustments to address new and important issues and constructive feedback from Fellows. Each year, Fellows meet in-person with officials and subject matter experts from across the U.S. Department of Energy, Office of the National Cyber Director, National Security Agency, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the U.S. Secret Service. Fellows also engage with Idaho National Laboratory researchers – about which one Fellow commented, "I learned a lot about the labs and the research they do, which exceeded what I hoped would happen." And in both 2022 and 2023, participants had virtual interactions with experts from the Transportation Security Administration (TSA). Building on this success, program staff anticipate in-person engagements with TSA in 2024. During these engagements, the Fellows reflect to agency briefers their perspectives and insights as critical energy infrastructure OT cybersecurity experts, helping to inform efforts that extend across the entire sector and critical infrastructure more broadly.

The maturation of the curriculum has allowed both the program staff and the Fellows themselves to focus on greater opportunities for intra-sector collaboration. This relationship building and information exchange among Fellows and their organizations is a concrete value to the participants. "My network has grown considerably," one Fellow explained. "I've taken a lot of notes and created personal action items to follow up on topics we discussed or approaches I heard others are taking that might help us improve."

While previous cohorts have also emphasized the importance of this aspect of the program, the 2023 Cohort created a novel mechanism towards the end of their year that they are continuing into the alumni program. In the vein of a crowdsourcing initiative, the Fellows identified dozens of topics of shared interest and concern, deciding on volunteer discussion leaders to brief on their organization's approach, and are collectively identifying best practices, recommendations, and reference guides. Topics of discussion have included asset management, remote access, threat detection in OT environments, and threat hunting for malicious and persistent threat actors like Volt Typhoon. A priority for the 2023 Cohort as they graduated from the OTDF was to encourage the next cohort to reach the level of trust and openness necessary for these conversations more quickly.

The Fellows have consistently underscored the value of the program and urged CESER to continue this initiative. One Fellow commented, “Please keep this program going. I feel there needs to be someone from each level of Energy (cooperative, IOU [investor-owned utility], public power, ONG [oil and natural gas]) in each state should go through this program. There is so much knowledge gained that it should be shared across the entire industry.”

The OTDF program has focused on providing value in three specific areas: 1) facilitating intra-sector collaboration, relationship building, and information exchange; 2) helping participants understand the context behind cyber threat information from the government; and 3) offering participants exposure to federal agencies and research conducted at national labs. The following memo outlines where the program is achieving these objectives and where the program can continue to be improved.

Finally, during the 2023 calendar year, the OTDF program hosted the first OTDF alumni session at Oak Ridge National Laboratory (ORNL). While a full assessment of the lessons learned from that session is beyond the scope of this memo, it is worth noting that because of the positive feedback to the ORNL experience and the 2023 Cohort’s crowdsourcing effort, program staff are expanding the alumni conference to include more time at the lab as well as ample time for in-person crowdsourcing discussions.

OTDF Provides Context and Facilitates Relationships

A founding goal of the OTDF program is to help participants gain a greater understanding of the federal agencies with equities in the cybersecurity of critical energy infrastructure. At the time of the program’s founding, there were limited programs geared towards improving public-private collaboration on OT cybersecurity. While the ecosystem continues to evolve with President Biden’s industrial control systems cybersecurity 100-day initiatives, efforts within CISA’s Joint Cyber Defense Collaborative, and the development of CESER’s Energy Threat Analysis Center, the OTDF continues to uniquely help Energy Sector participants understand and gain a greater contextual awareness of the federal government’s roles and responsibilities.

Fellows are drawn to the program in part because of this component of the OTDF. When asked about their expectations for the program, one Fellow expressed that they expected to gain a “better understanding of government offerings and establishment of partnerships with government entities like DOE, DHS, FBI, NSA, etc.” Another Fellow commented that after the program, “I feel very comfortable in my understanding about the roles DOE, DHS, FBI, and NSA play and who we can partner with for various needs.” A third Fellow echoed, “Understanding the functions that the FBI performs in comparison to what CISA provides helped clear up some confusion I had.”

As early as the first year of the Fellowship, it became clear that one of the most valuable aspects of the program was the unique intra-sector collaboration that the program fostered. One Fellow noted, "I learned a lot from hearing how others in the room would respond to those situations." Others similarly commented that peer relationships are some of the most valuable take-aways from the program. One stated, "Having a cohort of people in similar positions gives me a group to poll about 'how are you handling X?' or 'have you seen Y?' If the peer group can be kept together it is going to be a significant resource to pull from that will materially affect my organization's security."

While the Fellows represent diverse companies, many of the cybersecurity challenges they face are remarkably similar. One Fellow noted, "I personally learned a lot about how everyone is approaching risk and their defense strategy. I plan to implement as much as I can back in our organization with the realization that I do not have the same resources as larger entities." Another similarly observed, "Hearing about all the ways the larger companies reacted to regulatory requirements was eye opening."

During previous years, program staff had scheduled time for formal and informal discussions among the Fellows, but the 2023 Cohort pushed for even more self-directed, structured discussion time. "Our cohort wanted more time in our schedules for facilitated discussion and opportunities to learn from each other's experiences. The OTDF leadership team did well to re-arrange things to allow for it in Sessions 3 and 4," a Fellow commented. These structured discussions have since become monthly virtual discussions among the OTDF alumni across all three previous cohorts.

As in years past, CESER worked to facilitate security clearances through CISA's private sector clearance program for Fellows who did not already have a security clearance. While this is a significant undertaking and resource requirement for DOE and CISA, the Fellows have shared the value of understanding classified information for context in prioritizing and ensuring effectiveness of risk mitigation actions, as a result of participating in classified discussions. Receiving briefings and discussing classified threat information with the intelligence community partners, "gave better context on several reports that were released," one Fellow said. Another commented, "We were able to get to the meat of things, which I greatly appreciated." A third Fellow said that the classified brief and discussion "was far and away the most relevant and useful information to inform my day-to-day job. That kind of specific information about a specific incident or threat can be used (without detail/attribution) to directly inform security approaches and strategies in industry. It helps us understand what to look for and/or avoid."

Multiple Fellows also noted that since these briefings, conversations with local FBI field offices and fusion centers have been robust. Other Fellows noted that within their organizations, non-cyber personnel often are the ones with security clearances but ensuring that someone on the OT cybersecurity team has a security clearance improves information sharing. Fellows shared lessons learned and recommendations with each other on ways to get the most out of having a security clearance.

Finally, the 2023 Cohort also used their security clearances to have conversations with CESER leadership about the efficacy of the OTDF program. While this particular conversation did not have classified information, hosting the discussion in a secured space provided the opportunity for the Fellows to talk more openly.

OTDF Can Do More To Help Expand Government Understanding of Energy Sector Considerations

Even as the Fellows have consistently affirmed that the OTDF curriculum provides a well-rounded education about U.S. government stakeholders, they have also offered constructive feedback to ensure that the bidirectional discussions between federal agencies and Fellows are most constructive. The Fellows appreciated the read-ahead materials provided by Idaho National Laboratory prior to session 1 and encouraged program staff to provide similar pre-briefs ahead of interactions with federal agencies in sessions 2 and 3. They noted that this "homework" would enable them to begin to think about questions and discussion points in advance. Program staff are working with agency partners to respond to this feedback, in some cases relying on written materials. In others, program staff are scheduling short, virtual, pre-meetings between Fellows and agency officials to provide some introductory information in advance of in-person meetings.

Fellows also observed to program staff that some briefing topics were less relevant than others and that some presenters seemed more comfortable briefing than engaging in a discussion. In some instances, this feedback is helping program staff work with agency partners to adjust or refine the briefing and discussion topics for future cohorts. The OTDF participants are a unique group of highly technical experts, unlike other industry groups that agency experts may interact with on a more regular basis. Some agency partners may be more familiar with government affairs personnel, c-suite leadership, or even IT cybersecurity teams. The OTDF program, however, can help federal partners understand the unique needs, capabilities, and backgrounds of critical energy infrastructure OT cybersecurity professionals. Program staff will use pre-briefings and planning meetings with agency partners to encourage presenters to think through how they want or expect Fellows to use the information they are sharing.

A founding principle of the OTDF program is the importance of bidirectional information exchange between the federal government and the Energy Sector. In its first years, the OTDF focused particularly on ensuring that industry participants gained a greater understanding of federal government equities and capabilities and had opportunities to share their own knowledge and unique perspectives with government interlocutors. Having solidified a program to achieve these objectives, OTDF program staff solicited ideas from the 2023 Cohort about how the Fellowship might better serve agency partners as part of the core mission of the program. Offering opportunities for agency partners to seek feedback from the Fellows on research or programmatic efforts is useful but not sufficient for enabling other federal agencies to benefit from the deep expertise of OTDF participants.

Fellows commented that just as they gained a greater understanding of the federal government through interactions with agency personnel, federal agencies would gain greater insights into the day-to-day operations of OT systems and cybersecurity capabilities (and limitations) through on-site engagements with critical energy infrastructure owners and operators. Through direct relationships with FBI field offices, CISA regional offices, and other federal, state, and local governments, some OTDF alumni are already hosting such engagements. Some of these relationships are the direct result of OTDF engagements. Leveraging the ideas, insights, and feedback of the 2023 Cohort, OTDF program staff are exploring how the Fellowship could amplify and expand, formally or informally, upon these individual initiatives.

While anecdotal, a member of the FBI's cyber action team confirmed the potential value of such opportunities after witnessing a portion of the discussion during the session 4 capstone exercise. The capstone provides Fellows an opportunity to practice decision-making skills and critical thinking in a series of realistic situations related to defending OT against cyber threats. The FBI agent witnessed the discussions among the Fellows after a series of injects presented anomalous activity in OT environments but before any determination had been made that there had been a cyber incident. The agent commented that they did not previously have an appreciation for all of the investigation, analysis, and decision making that occurred before companies called the FBI to report a cyber incident. OTDF program staff are seeking ways to replicate this experience for other agency partners.

Conclusion

With three years of data, the conclusion is clear: CESER's Operational Technology Defender Fellowship is a valuable program for OT cybersecurity managers across the Energy Sector. Fellows and alumni are implementing lessons they learn and using knowledge they gain to improve the cyber resilience of critical energy infrastructure.

While some Fellows applied to the OTDF after seeing information that CESER shared with industry groups for distribution, multiple members of the 2023 Cohort noted that they applied because a trusted colleague previously participated and encouraged them to do so. This word-of-mouth advertising is encouraging and indicates that CESER can depend on not only formal information sharing mechanisms but also informal networks of trust to scale the lessons from the OTDF to the broader Energy Sector.