Observations, Insights, and Lessons Learned from Cohort 2022

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. OT Defender Fellowship (OTDF) participants gain a greater understanding of the OT threat landscape and strengthen their capabilities to defend critical energy infrastructure. The full agendas for the four sessions are included as Appendix A.

In its first year (2021), the OTDF operated in a hybrid model with limited in-person opportunities. In 2022, the program held the four in-person quarterly sessions as originally envisioned. Programmatically, the Fellowship matured significantly over 2022 with the solidification of the curriculum and the build-out of virtual intersessions that facilitate regular opportunities for further engagement with U.S. government experts. The program staff has found willing partners at other agencies who have helped ensure bidirectional, technical, frank, informative conversations. Even the National Security Agency (NSA) — which does not have direct responsibility or authority regarding critical energy infrastructure — demonstrated to the Fellows that across the board, the U.S. government desires and indeed requires robust engagement with the private sector.

The OT Defender Fellowship is also developing programming for alumni. The 2021 and 2022 cohorts overlapped at their Sessions 4 and 1, respectively, at Idaho National Laboratory (INL) in March 2022, which allowed the 2022 Fellows to build peer-to-peer relationships with alumni. This overlap was a scheduling anomaly and not a deliberate feature. However, due to the collaboration benefits of this happy accident, opportunities for alumni to interact with the current cohort are now a regular feature. Alumni not able to attend their own capstone session joined the following year, and alumni have participated in select intersessions and portions of in-person programming.

Throughout the year, the Fellows shared their OTDF experiences in industry meetings and conferences, and OTDF staff were invited to brief industry groups about the program. The reception at each of these briefings has been extremely positive. The program was also featured in an article in the Edison Electric Institute's (EEI) Electric Perspectives magazine, praising the program for providing "security managers access to a useful and unique information-sharing process, enhanced by a wide variety of participants who offer their own diverse perspectives on critical security issues."[a]

For Fellows, the value of the OTDF is three-pronged: 1) the Fellowship provides greater understanding of the security and operational challenges and opportunities; 2) it creates

[a] https://cdn.coverstand.com/6643/755606/33fc8203fbc9a45c883fa913304bc535f815c8c7.pdf

connections with and understand of government agencies with equities in the sector; and 3) it fosters relationships among participants.

Of the program, one Fellow commented:

> "I would like to state that this is by far the best opportunity I have had in my professional career to date. The exposure and information gained has greatly benefited me personally, professionally and the knowledge I can bring to my organization. The Fellowship has brought me closer to the Energy Sector with more meaningful professional connections and friends that I can trust with sharing information, exposure of programs, government insight and industry best practices that are actually working in live environments."

While the Fellows and programming staff have identified areas for improvement in the curriculum for the 2023 Cohort, these have mostly been minor adjustments rather than major overhauls. Fellows themselves are eager to assist with the refinement of the program. One Fellow noted, "I would love the opportunity to be part of the continued formulation … I see all kinds of opportunities with this program."

The following report outlines where the program is hitting the mark by meeting or exceeding the expectations of participants, and where there are opportunities for refinement of the program to better achieve desired outcomes. Perhaps the most frequent theme throughout the discussions was the challenge of managing third-party risk from suppliers. For this reason, the final section of this report provides the Fellows' collective perspective on the importance of minimum-security requirements for critical infrastructure vendors.

OTDF Provides Unique Opportunities for Information Sharing and Relationship Building

Fundamentally, the Fellows expected the program to provide "more than we can Google or read in the newspaper." Fellows admitted they anticipated a series of government PowerPoint presentations but were pleasantly surprised the program pushed partners to engage in bidirectional discussion (usually successfully). Deeper insights into both challenges and opportunities are indeed what the Fellowship strives to provide. One Fellow noted:

> "The OT Defender Fellowship provided a behind-the-scenes view of key OT cybersecurity programs. In some cases, it looks confusing from the outside because it is in fact confusing. There were several programs that hearing these presentations allowed me to determine either 1) we needed to engage or 2) this program would not be a fit for my organization."

The Fellows were particularly appreciative of the discussions with DOE CESER personnel about the Infrastructure Investment and Jobs Act, which provides multiple buckets of funding through DOE and CISA (Cybersecurity and Infrastructure Security Agency) to improve the cybersecurity of critical energy infrastructure. One Fellow commented these discussions were "useful and exactly what we had hoped for."

A core component of the Fellowship is providing the participants with exposure to the broad array of government agencies with equities in cybersecurity of critical energy infrastructure. One Fellow noted he was "incredibly impressed with the level of access to the variety of organizations." Another commented that relationships between government and industry are "invaluable." Still a third said:

> "The experience to sit in front of and with open direct access to so many United States Government officials and departments with the opportunities to have open Q&A sessions with them was an experience that will probably never happen at that level again in my career."

The Fellows also remarked that they appreciated learning what the federal government is doing to help critical energy infrastructure owners and operators improve cyber resilience and respond to cyber incidents, and that this component of the program exceeded expectations. The Fellows gained a greater understanding of CISA's roles in asset response, the FBI's capabilities in threat response, and of the unique role of DOE as the energy sector's risk management agency. They also gained a greater appreciation for how their organizations might interface with different parts of the federal government if they need different types of assistance. A Fellow commented, "knowing who is involved and who to reach out to in a time of need is half the battle."

Over the course of the 2022 OTDF program, the Fellowship provided unique opportunities to contribute to ongoing discussions regarding improving national cyber resilience. The Fellows met with congressional staff and with leadership from the Office of the National Cyber Director to discuss the direction of national cybersecurity policymaking. The Fellows also contributed feedback to CISA's efforts to develop the first version of its Cybersecurity Performance Goals (CPG).

The most consistent comment from the Fellows was a deep appreciation for the level of camaraderie the program helps facilitate among participants, noting it even exceeds that within other industry-led collaborative undertakings. "Having peers to bounce ideas off of, validate your thinking, and to learn how they are solving similar problems is of highest return," a participant explained.

The program achieves this through both structured and unstructured opportunities for participants to exchange ideas and best practices. "I expected there to be networking and all that, but that was actually much more beneficial than I ever expected given the diversity of the Fellows," one Fellow commented. Another noted, "The relationships that have been developed will be beneficial for many years."

Participants appreciated the fact the Fellowship draws from across the Energy Sector and strives to have a diverse representation of companies and individual backgrounds, while

maintaining an intimate nature. This is one of the appeals of the program, as one Fellow noted: "I knew that I was kind of in my own little [company] bubble, and I wanted to be able to connect with others and compare notes. … That's been immensely beneficial." Others noted they are already leveraging these new relationships with their peers and government partners.

Alumni Engagement and Marketing Are Areas For Continued Growth

The Fellows provided staff with constructive feedback to continue refining the curriculum. While the Fellows appreciated the exposure to the wide range of USG programs, they encouraged the prioritization of particular programs with direct relevance and wanted additional time in classified discussions. They offered suggestions that program staff have relayed to interagency partners and have used while building the 2023 syllabus. They also suggested the Fellowship should provide an opportunity to review foundational, read-ahead materials to allow greater time for discussion. Program staff had been hesitant to put additional demands on Fellows' time, but participants allayed these concerns.

The Fellows also encouraged program staff to build-out the alumni programming. They suggested organizing alumni visits to other national laboratories to provide participants with even broader exposure to the research that DOE is undertaking to improve the cybersecurity of critical energy infrastructure. Program staff acted on this idea in 2023, hosting the first alumni in-person session at Oak Ridge National Laboratory in August. Given the positive response from that engagement, similar events will likely become a cornerstone of the alumni program.

Outside the Fellowship itself, participants identified growth areas for broader public-private collaboration. While addressing these concerns is outside the scope of the Fellowship, the feedback is included in this report because it provides useful insights program staff use while refining the syllabus for subsequent cohorts and for the alumni program.

The 2022 Cohort coincided with national conversations about cyber incident reporting and the need for harmonization of reporting requirements. Fellows remarked on the desire for regulators to have consistent reporting requirements and a clear definition of what the USG considers to be a cyber incident for the purpose of reporting. In an ideal world, there might be a common call center that would provide companies with a simple explanation of "here is what you do and who you call." Fellows observed policy trends towards greater reporting, but questioned what value asset-owners might eventually gain from this aggregated and analyzed data.

More broadly, the Fellows noted asset-owners are providing information to the USG, but typically do not receive any specific feedback on how their information was used. The Fellows noted that some of the negative feelings around information sharing might be

mitigated with a clearer articulation of why the government wants the information and how it anticipates others in private industry will benefit from its sharing.

Supply chain fragility and third-party security continued to be a concern for the 2022 Cohort. This appears to be one of a couple areas where government and private sector partners have mismatched expectations about the capabilities of the other to sufficiently address the problems. Fellows expressed frustration that every company is trying to do due diligence and vendor assessments independently, noting this is an inefficient and likely ineffective approach to security. As discussed in the next section, the Fellows repeatedly expressed a desire for the USG to articulate minimum standards or possibly regulations for critical infrastructure vendors. The Fellows urged government partners that the message ought to be that vendors need to take greater responsibility for cybersecurity rather than putting the onus entirely on the end-user.

OTDF Participants Offer Unique Perspective on Vendor Obligations

The 2022 Cohort coincided with increasing USG efforts to impose minimum security requirements on critical infrastructure owners and operators. The Fellows represent companies that generally have relatively mature cybersecurity postures, a majority of whom come from a subsector with mandatory cybersecurity regulations already in place for more than a decade (bulk electric power). As professionals responsible for the security and reliable operation of OT equipment, the Fellows believe strongly in the importance of critical infrastructure cybersecurity. While the Fellows expressed reservations about some aspects of the government's execution, they agree with the intent.

One of the concerns most consistently raised throughout the program was third-party risk. Fellows expressed concerns about the security of the equipment they are adding to their OT and IT systems and believe there are insufficient requirements on vendors to produce secure products. Under the current regulatory climate, security requirements fall on the asset owners and operators, not on the equipment manufacturers. This system is inefficient, unsustainable, and unlikely to produce the best overall security.

As a proposed solution, the Fellows offered a set of minimum-security requirements for critical infrastructure equipment providers. The Fellows emphasized that any new requirements should leverage existing standards and be simple enough that companies of all sizes and cyber maturity levels can understand the rubric. Fellows explained that comparing two products (from a security perspective) should be as simple as reading the nutrition labels on cans of soup.

The following list outlines the types of high-level behaviors Fellows would like to see as the basis of the requirements:

- Adherence to principles such as Cyber-Informed Engineering and secure-by-design, meaning security is built into the product rather than tacked on later.
- Adherence to principles such as security-by-default such that features are configured for maximum security as the default setting off-the-shelf and prompt default passwords be changed upon initial configuration.
- Ability to support strong authentication with long and complex passwords and multi-factor authentication.
- Attestation or other demonstration of secure software development practices.
- Provide Software Bills of Material and Hardware Bills of Material, and actively communicate newly discovered vulnerabilities and their remediations.
- Commitment from the provider to address security vulnerabilities including in the device firmware for the full lifespan of the product.
- Ability for asset owners and operators to securely update devices, and for the use of additional or compensating security controls to not invalidate warrantees.
- Sourcing / building all critical components domestically or in non-adversarial foreign countries.
- Use of strong encryption algorithms and the ability to upgrade this encryption as new standards become available.
- Use of standard protocols (rather than proprietary protocols) that operate with security-by-obscurity.

Conclusion

Responses from Fellows throughout 2022 reaffirmed the value of and need for the OT Defender Fellowship. Constructive feedback will continue to help the program staff refine the curriculum for future cohorts and expand alumni opportunities.

As is often remarked, cybersecurity is a team sport. The OT Defender Fellowship is helping to create trust and relationships across the Energy Sector and between industry and government. These relationships are essential for collaboration and coordination to strengthen and secure U.S. critical energy infrastructure.

Appendix: Session Agendas

Session 1 (Idaho National Lab)

March 30, 2022

- Fellowship Goals and Intent *with Brian Marko (Program Manager, Energy Sector Exercises Program, DOE) & Samantha Ravich (Chair, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies; Commissioner, U.S. Cyberspace Solarium Commission)*
- Fellow Introductions
- Agenda Review and Objectives *with Jared Smith (Program Manager, Idaho National Laboratory)*
- Welcome and INL Overview *with Zach Tudor (Associate Laboratory Director, National and Homeland Security)*
- U.S. DOE / Idaho National Laboratory Cyber Projects *with Virginia Wright (Energy Cyber Portfolio Manager, INL)*
- CIC Facility and Lab Tours *with Scott Cramer (Director, Cybercore Integration Center, INL); CyTRICS Lab: Virginia Wright; Malware Lab: David Hudson (Program Manager, INL); University Lab: Eleanor Taylor (Program Manager, INL); OpDefender and Power Lab: Briam Johnson (Chief Power Engineer, INL)*
- INL Cyber-Physical Test Pads; *Test Pad A and Obsidian Test Pad: Carla Heathman (Power Systems Engineer, INL); Test Pad D: Jake Gentle (Project Manager, Infrastructure Security & Renewables, INL); Wireless Test Range Tour: Scott Peterson (Program Manager, Wireless Test Bed, INL) & Brad Nelson (Energy Sector Communications Program Lead, INL); Experimental Breeder Reactor I Tour: Shelly Norman (INL Ambassador)*

March 31, 2022

- Introduction to the CyberStrike Workshop *with Dan Noyes (Program Manager, INL) & Tim Conway (Subject Matter Expert, SANS Institute): Introduction and overview of the Ukraine Cyber Attacks and include lab exercises focusing on: Open-Source Reconnaissance, Controlling the HMI, and Denial of Service. Key topics areas include Adversary TTPs*
- Landscape: Connecting the Dots *with Sam Chanoski (Technical Relationship Manager)*
- Electric Vehicle Infrastructure Lab (EVIL) Tour *with Richard "Barney" Carlson (Principal Research Engineer, INL)*

- CyberStrike Workshop: *Lab exercises focusing on Bypassing the HMI, Firmware Analysis, Passive Man in the Middle, Active Man in the Middle, and Network Segmentation. Key topics areas include Adversary Operations and Capabilities, Force Multipliers and Effects, Guidance and Mitigation Concepts, Attack Prevention Techniques, and Defending the Effect*

April 1, 2022

- Course: Principles of Cyber-enabled Sabotage and Engineering Protections *with Curtis St Michel (Technical Director, INL)*
- Roundtable Discussion *with Sam Chanoski (Technical Relationship Manager, INL)*
- Controls Environment Laboratory Resource (CELR) Tour *with Jason Maughan (Program Manager, INL)*
- Cybersecurity Analysis Center (CSAC) Tour *with Kelly Johnson (CSAC Lead, INL)*
- Cyber-CHAMP Program Briefing *with Shane Stailey (Program Manager, INL)*
- Session Wrap-up *with Brian Marko (Program Manager, Energy Sector Exercises Program, DOE) & Jared Smith (Program Manager, INL)*

Session 2 (Washington, DC)

June 28, 2028

- Opening Remarks/CISA Cybersecurity Division Overview
- Joint Cyber Defense Collaborative *with Seth McKinnis & David Forscey (JCDC Operational Planning): Discussion topics included How to become a JCDC member, the ICS specialist group, and the pipelines project*
- Vulnerability Management: Operational Resilience *with Steve Pozza (VM Assessments, Operational Resilience): Discussion topics included Validated Architecture Design Review (VADR) Assessment Overview, Lessons Learned, Aggregated Observations, and Best Practices for Architecting Resilient Systems*
- Threat Hunting: Incident Response (Asset Response) with Jeff Rabinovitz (Acting Section Chief, *Threat Hunting, ICSS)*
- Threat Hunting: Incident Response (Technical) *with Shaun Long (Threat Hunting, ICSS) & Carol Sledge (CyberSentry)*
- VM Insights Overview with Chris Hild & Gabriel Davis (*VM Insights)*
- Vulnerability Management: Disclosure with Lindsey Cerknovik, Iain Deason, & Martin Kihiko (*VM Disclosure). Discussion topics included* What do asset-owners need to know and what should they expect from CISA?

- CISA's Cybersecurity Division Strategic ICS Efforts with Sarah Beckel, Peter Colombo, & Rachel Russo (*Office of the Technical Director): Discussion topics included the* Cybersecurity Performance Goals, Sector 100 Day Plans, and ICS Vision and Long-Term Strategy
- Threat Hunting Deep Dive with David Hudson (*Idaho National Labs)*

June 29, 2022

- Overview of the Office of the National Cyber Director *with Rex Booth (Director, Stakeholder Engagement)*
- ONCD Priorities Briefing *with Neal Higgins (Deputy National Cyber Director for National Cybersecurity)*
- Q&A/Roundtable Discussion
- Background On the Cybersecurity Performance Goals *with Peter Colombo & Rachel Russo (Cybersecurity Directorate (CSD) Office of the Technical Director): Discussion topics included National Security Memorandum-5, Cross-Sector and Sector-Specific Structure, and Timeline and Status*
- High Level Performance Goals Introduction, Discussion, and Feedback Session *with Peter Colombo & Rachel Russo (CSD Office of the Technical Director)*

June 30, 2022

- Welcome, Cybersecurity Collaboration Center (CCC Overview and Industry Collaboration *with CSD Senior Leadership Engagements, CCC Engagements and Upskilling Team, CSD Technical Director, & Defense Industrial Base Chief, CCC: Discussion provided an overview of CCC, how industry partnerships are used to fuse Signal Intelligence (SIGINT) leads with commercial data and insights from commercial partners to detect the adversary, create innovative, new tradecraft to discover and track adversaries threatening these networks, and mitigate threats through collaborative development and sharing of mitigation guidance that amplifies the NSS and DIB's ability to prevent and eradicate threats.*
- NCS/Strategies for Information Sharing with CISA Senior Liaison & Capabilities Directorate Control Systems Defense Expert: Discussion focused on private industry's views on key issues and critical partnerships that still need development, lessons learned from other agencies, and strategies for information sharing.
- Roundtable on "What Keeps You Up at Night" with *CISA Senior Liaison & Capabilities Directorate Control Systems Defense Expert*
- Lessons Learned & Supply Chain Threats Roundtable *with CSD Technical Director & CISA Senior Liaison*

- Cyber Threat Briefing & Key Intelligence/Regional Info Sharing *with Civilian CSD & other experts: Discussion topics included reviewing cyber threats at an unclassified level, various device and system vulnerabilities, advisories, and investigations, and improved intelligence supporting OT cybersecurity.*
- SCADA Lab Tour
- Enigma Demo

Session 3 (Washington, DC region)

September 20, 2022

- Welcome, CESER Initiatives & Priorities *with Monica Neukomm (Acting Principal Deputy Director)*
- Infrastructure Bill Discussion *with Monica Neukomm (Acting Principal Deputy Director), Cynthia Hsu (Cybersecurity Specialist), & Mike Toecker (Cybersecurity Advisor)*
- Intelligence Division Overview & Threat Briefing *with Tony Waylonis (Cyber Intelligence Division, DOE Office of Intelligence and Counterintelligence) & Matt Tarduogno (CESER Program Manager)*
- Roundtable discussion *with Brian Marko (Program Manager, Energy Sector Exercises Program) and Frank Honkus & Tyler Tiller (E-ISAC): Discussion topics included workforce provisions in the infrastructure bill and information sharing*
- Cyber Response Programs *with Matt Tarduogno (Program Manager)*
- Risk Management Tools and Technologies *with Jessica Perry (Threat Mitigation Program Manager)*
- Fellows Roundtable and White Board Session

September 21, 2022

- Welcome to FBI Quantico
- Cyber Action Team (CAT) & Incident Response *with Michael Thomas*
- FBI Roundtable Discussion
- Behavioral Science Unit
- FBI History, Academy and Training Tours *with James Ruby & Training Instructors*

September 22, 2022

- Welcome and FBI Cyber Mission *with Scott Ledford (Unit Chief, Technical Operations, Cyber Division)*
- Capabilities and Interagency Coordination *with National Cyber Investigative Joint Task Force & Gabe Maxwell (Technical Operations, Cyber Division)*
- ICS Threat Briefing & Cyber Engagement *with Kermie Bledsoe (Intelligence Analyst)*
- Roundtable: What Keeps You Up at Night?
- Congressional Briefing *with Evan Burke (Legislative Assistant to Rep. Jim Langevin (D-RI))*
- Capitol Hill Tour

Session 4 (Florida Power & Light)

December 6, 2022

- Arrival and Welcome *with Christopher Strain (OTDF 2021 Alumnus, Director of Technical Risk Management, NextEra)*
- Session Agenda Review and Objectives *with Marcela Stacey (Program Manager, INL)*
- Cyber Protective Mission *with Scott Reed (Supervisory Special Agent & Program Manager, U.S. Secret Service) & Sam Messinger (Supervisory Special Agent, Critical Systems Protection Program, U.S. Secret Service)*
- Capstone: Scenario 1, Increased Geopolitical Tensions *with Sam Chanoski (Technical Relationship Manager, INL) & Carla Heathman (Principal Researcher and Power Engineer, INL)*
- Site Visit: Distribution Control Center, Storm response

December 7, 2022

- Capstone: Scenario 2, Impact and Immediate Response *with Sam Chanoski (Technical Relationship Manager, INL) & Carla Heathman (Principal Researcher and Power Engineer, INL)*
- OTDF Program Findings Discussion with Annie Fixler (Deputy Director, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies)
- Site Visit: PGA Building, Drone Control Center

December 8, 2022

- Capstone: Scenario 3, Consequence Management and Alternatives Response *with Sam Chanoski (Technical Relationship Manager, INL) & Carla Heathman (Principal Researcher and Power Engineer, INL)*

- Capstone Feedback Response *with Sam Chanoski (Technical Relationship Manager, INL)*
- Discussion with System Control Center team
- Site Visit: Systems Control Center
- Fellowship Wrap-up, “Graduation” and Next Steps