Executive Summary

Cohorts 2021, 2022, and 2023

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

Idaho National Laboratory

History and Mission

Protecting the nation's energy infrastructure from modern threats is critical to national security. Security managers play a decisive role in defending the critical energy infrastructure against ubiquitous cyber threats, cyber-enabled sabotage, and physical security breaches. Their work bridging executive intent and technical reality is both important and challenging – but the necessary resources are often limited.

To better support these front-line leaders, U.S. DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) created the Operational Technology Defender Fellowship (OTDF). This program offers middle to senior-level operational technology (OT) security and operations leaders across the U.S. Energy Sector an opportunity to understand high-level strategies and tactics adversarial state and non-state actors use in targeting U.S. energy infrastructure as well as the roles and capabilities of U.S. departments and agencies to support critical infrastructure owners and operators.

The year-long fellowship offers a bidirectional information and idea exchange forum between government and Energy Sector experts, contributing to the collective advancement of cybersecurity and information sharing capabilities and processes that will endure beyond the end of their cohort. The Fellows regularly engage with subject matter experts from across the U.S. Department of Energy, Office of the National Cyber Director, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), Transportation Security Administration, Federal Bureau of Investigation (FBI), and the U.S. Secret Service.

Over the course of four in-person, week-long sessions and multiple virtual intersessions, the program also seeks to facilitate and expand peer-to-peer relationships among cohort members for the long term, to share ideas, validate thinking, and problem-solve similar challenges. Within the program, participants exchange insights and perspectives on the current state of cybersecurity operations, capabilities, gaps, constraints, and areas for mutual improvement to better defend the nation's critical energy infrastructure.

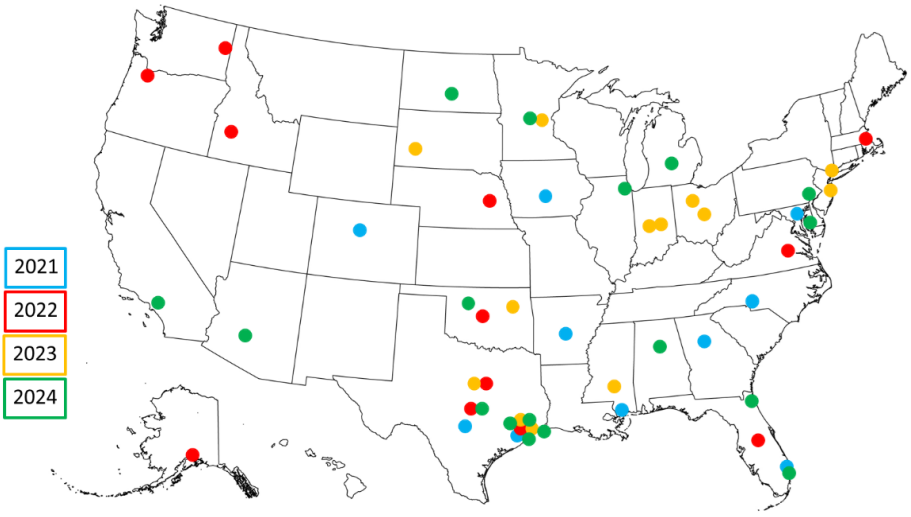
CESER created this program in the wake of the congressionally mandated Cyberspace Solarium Commission's urging the federal government to operationalize collaboration with the private sector. At the time of its founding, there were limited programs geared towards improving public-private collaboration on OT cybersecurity. Over the past three years – and as the fourth cohort of Fellows begins their program – OTDF has provided opportunities for critical energy infrastructure OT experts to contribute their insights to federal government cybersecurity efforts like the President Biden's-sponsored Industrial Control Systems Cybersecurity Initiative, CISA's Critical Infrastructure Cybersecurity Performance Goals, the Rural and Municipal Utility Cybersecurity grant program, and cybersecurity workforce development efforts.

"This is by far the best opportunity I have had in my professional career to date," one Fellow remarked. "The exposure and information gained has greatly benefited me personally and professionally, [providing] knowledge I can bring to my organization." With this kind of encouragement, OTDF has matured and expanded, bringing in a greater number of participants each year and developing an alumni program.

The Fellowship is sponsored by DOE and administered by Idaho National Laboratory with support from the Foundation for Defense of Democracies' Center on Cyber and Technology Innovation.

Program Growth Driven by Demands for More Intra-sector Collaboration

The Fellowship began as a pilot program with eight participants in its first year. While striving to maintain the intimacy and trust of small group collaboration, the program has accepted a greater number of participants each year. The 2024 Cohort now includes 18 participants. (See the map below identifying the geographic diversity of participating companies by cohort year)



As conceived, the program strives to select participants representing all parts of the U.S. Energy Sector, including electricity, oil, natural gas, and renewable energy companies. Participants hail from investor-owned utilities and cooperatives, publicly traded multinationals, and public power and municipally owned organizations. The discussions and networking were "much more beneficial than I ever expected given the diversity of the fellows all the way from oil to regional transmission organizations down to distribution. It was very nice having the whole picture represented." As a result, during the candidate selection process, OTDF prioritizes building the best cohorts with the priority focused on the diversity of technical and business experience.

Commented [MW1]: This could be misinterpreted and isn't needed to convey the point.

As each cohort has graduated from the program, they have sought to maintain the camaraderie and collaboration they found in the Fellowship. Initially, this took the form of Slack channels and informal meetups at existing industry conferences. At the suggestion of the 2022 Cohort, OTDF launched its own alumni session, visiting Oak Ridge National Laboratory in 2023 to engage with subject matter experts leading critical energy infrastructure cybersecurity research and programs. In 2024, Sandia National Laboratories will host the alumni session which will include not only meetings with lab researchers and classified briefings, but also an on-site visit to the operations facility of a local utility and ample time for discussion and collaboration across the alumni cohorts.

This cross-cohort, intra-sector discussion time has become a core component of the alumni program. Each year, Fellows have emphasized the value of the lessons exchanged among participants, asking for more structured and unstructured time for "Fellows-only" discussions. In the latter half of 2023, the Fellows launched a self-directed, structured effort to identify dozens of topics of shared interest and concern, selected discussion leaders to brief on their organization's approach, and collectively identify best practices, recommendations, and reference guides. This has adapted into a monthly, virtual roundtable series among the alumni that also includes representatives from various federal agencies whom they have met during their cohort years.

In addition to sharing lessons from OTDF with their organizations, Fellows have already briefed industry groups and associations about the program and its benefits for public-private collaboration and intra-sector collaboration. After exposure to specific training programs, Fellows and alumni have sent personnel from their teams to receive that training and have hosted related training programs at their own organizations. While expanding the number of Fellows in each cohort will be debated, the empowerment of the Fellows to continue sharing the knowledge gained within their organization and with the broader energy sector remains the priority for the program.

Lessons for Public-Private Collaboration

OTDF has helped Fellows experience and internalize the value of building relationships with federal, state, and local officials and law enforcement. After participating in the Fellowship, multiple Fellows have hosted delegations of FBI cyber experts to help their organizations gain a greater appreciation for the nuances and unique considerations of OT cybersecurity. One Fellow remarked, "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." After concluding the program, participants reported greater attendance of briefings at local fusion centers, noting that these have been "extremely valuable."

The increased interaction between Fellows and government officials has helped dispel misconceptions about other's capabilities and clarified the ways in which government can support the cybersecurity of critical energy infrastructure. Reflecting on their own assumptions, Fellows noted that, at times, both industry and government seem to believe

the other has extraordinary insights or unique capabilities they are unable or unwilling to share. This is the result, at least in part, of a lack of interpersonal trust that hinders efforts to build public-private collaboration between organizations. Direct interactions between critical energy infrastructure operators and government subject matter experts are part of the solution. One Fellow remarked that after OTDF, "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."

The Fellows also stressed to government leaders and staff the transformational nature of direct engagement between federal agencies and critical infrastructure owners and operators. During 2023, Fellows shared how much they appreciated the efforts of TSA (uniquely although not exclusively) to work with pipeline operators to refine the security directives.

The Fellows noted that the program helped them gain a greater understanding of CISA's roles in asset response, the FBI's capabilities in threat response, and of the unique role of sector risk management agencies. 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."

OTDF has also reinforced the value of exercising incident response plans and sharing after-action reviews and lessons learned. After achieving a level of trust among themselves, Fellows have been willing to share their own experiences in real cyber incident responses. One Fellow noted, "The discussions with my peers about their interactions with [government] agencies during an incident have led me to refine and modify my incident response plans."

Meanwhile, OTDF's Capstone Exercise itself forces participants to ask and answer difficult questions, reminding Fellows that they will often have to respond to potential incidents with incomplete information. The Capstone Exercise 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. It facilities discussion among the Fellows and highlights the different responses, for example, of small and large companies. Fellows have consistently validated the utility of this Capstone and other exercises that force participants to wrestle with imperfect decision making in incomplete information environments.

Finally, OTDF has shown the value of critical energy infrastructure operators understanding classified information for context in prioritizing and ensuring effectiveness of risk mitigation actions. Fellows noted that often within their organization, senior leaders and physical security managers have security clearances and receive briefings on classified information but not necessarily members of the OT cybersecurity team. Receiving classified briefs and engaging in discussions in classified settings provided "better context on several reports that were [publicly] released" and the "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." With their specific expertise, the Fellows were able to understand the OT cybersecurity implications of the information provided in classified settings in ways that other members of the same organizations might not have been able to.

Commented [MW2]: Want to emphasize it is about understanding classified information, not the clearance itself. That is the review process to allow you access.

Conclusion

More detailed accounts of the observations, insights, and lessons learned from the 2021, 2022, and 2023 cohorts of the DOE's Operational Technology Defender Fellowship are included in separate reports. The reports can be found at https://www.energy.gov/ceser/ceser-exercise-library.

CESER looks forward to continuing this important program and appreciates the commitment, collaboration, and expertise of the federal agencies and government leaders who have devoted their time and resources to the development of the program and accomplishment of its mission. OTDF's success is also due in large part to the investment of the Fellows and of their organizations to share valuable time and expertise. CESER thanks them for their commitment to the security and resilience of critical energy infrastructure.