Agency Priority Goal | Action Plan | FY 2023, Q1-Q2

Energy Sector Cybersecurity

Goal Leader(s):

Goal Leader – Fowad Muneer, Acting Deputy Director
Deputy Goal Leader – Stephanie Johnson, Ph.D., Program Manager

Goal Overview

Goal Statement

- Increase the overall cyber resilience of the grid by addressing critical cyber vulnerabilities prior to adversary exploitation through a multi-faceted approach that includes applying classified threat intelligence, illuminating systemic cyber supply chain risks, cyber vulnerability testing and forensic analyses, and engineering out cyber risks – all in close partnership with asset owners and manufacturers across the Energy Sector Industrial Base.

Problem to Be Solved

- Cybersecurity vulnerabilities in digital components in critical infrastructure are a growing concern as nation-state adversaries and cyber criminals seek to exploit these weaknesses. A key strategy in reducing potential consequences for critical infrastructure from these threats is to discover high-priority vulnerabilities and proactively work with impacted asset owners and manufacturers to address them before exploitation.
- Pursuant to direction in Sec. 40122 of the IIJA, the voluntary Energy Cyber Sense program increases the cyber resilience of energy sector systems by applying classified threat intelligence, identifying systemic cyber vulnerabilities through expert testing, and working with energy sector asset owners and manufacturers to address them.

What Success Looks Like (2-year goal)

- By September 30, 2022, analyze no less than 10% of critical components in energy sector systems; and expand manufacturers participating in the voluntary Energy Cyber Sense program to cover no less than 15% of the market share of critical components.
- Drive down overall cycle time for critical vulnerability discovery to mitigation to notification of impacted asset owners by at least 10%, compared to a 2021 baseline.
- By September 30, 2023, analyze no less than 15% of critical components in energy sector systems; and expand manufacturers participating in the program to cover no less than 30% of the market share of critical components.

Tracking the goal

Goal target(s)

Achievement statement		Key indicator(s)	Quantify progress			Frequency
By…	**We will…**	**Name of indicator**	**Target value**	**Starting value****	**Current value**	**Update cycle**
09/30/23	Manufacturers representing 30% of critical components in energy sector systems are voluntary program participants	Manufacturers Participating	30%	0%	34%	biannually
09/30/23	10% of critical components have undergone testing	Critical Components Tested	10%	0%	Between 11.7% and 47%*	biannually
09/30/22*	**Cycle time from vulnerability discovery to mitigation is reduced by 10%**	**Cycle Time**	**10%**	**17 months**	**5 months/71%**	**annually**

* The stated range reflects three different methods used to calculate the number of critical components that have undergone testing in the CyTRICS program.

1. Coverage of Critical Components analyzed with respect to an Energy Sector Reference Architecture
    a. CyTRICS analyzed 5 out of 12 types of critical devices reflected in the reference architecture, or 41.6%
2. Coverage of Critical Components analyzed with respect to a program-generated List
    a. CyTRICS analyzed 2 out of 17 devices on a list of critical components generated by National Laboratory power system subject matter experts in 2020, or 11.7%
3. Coverage of Critical Components as assessed by a market research company
    a. CyTRICS commissioned an independent market research company, Newton-Evans, to estimate the percentage of the U.S. market segment represented by devices tested under the program, which was 12% as of 2022

The program took this approach because it is not possible to measure progress towards the APG based on the actual deployment of specific systems within the energy sector, since asset owners hold the specific constituency of assets deployed as protected information.

Goal Team

Program Management (CESER)
- Program Lead – Stephanie Johnson, Program Manager

Lab Performers
- INL Program Manager – Ginger Wright; Principal Investigator – Robert Erbes
- SNL Program Manager – Rob Kaack; Principal Investigator – (vacant)
- LLNL Program Manager – Robert Hanson; Principal Investigator – Steve Chapin
- PNNL Program Manager – Jess Smith; Principal Investigator – Lucas Tate
- ORNL Program Manager – Jeff Schibonski; Principal Investigator – Jason Carter
- NREL Program Manager – Jon White; Principal Investigator – Zoe Dormuth

Industry Partners
- Schneider Electric
- Hitachi Energy
- Schweitzer Engineering Labs
- Southern Company
- New York Power Authority
- GE Research (pending)

Goal Strategies

- Continue to sign participation agreements with asset owners and manufacturers to increase access to critical components for cyber vulnerability testing
- Define baseline testing capabilities and capacity at 6 National Labs; assess capabilities against requirements
- Validate criticality of components using a variety of inputs including classified threat intelligence and a bespoke prioritization algorithm
- Baseline market coverage for critical components using a variety of inputs including market data, manufacturer information on market share, and asset owner reporting on installed base
- Baseline cycle time for cyber vulnerability and mitigation cycle; initial proof of concept was >17 months

Key milestones

- Activities conducted under the Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program will be leveraged as an element of the new Energy Cyber Sense Program established under IIJA Section 40122 which became law during Q1 of FY22.
- Milestones reflect direction envisioned under the broader Energy Cyber Sense Program.
- Activities may be adjusted due to emerging policy direction under E.O. 14017, “America’s Supply Chains,” and other supply chain-related executive orders.

Milestone Summary

Key Milestone	Milestone Due Date	Milestone Status	Change from last quarter	Comments
Develop a Strategic Plan for the Energy Cyber Sense program	03/31/22	*Complete*	No change	Complete.
Draft an Initial Test Process to be leveraged by the program and, pursuant to Sec. 40122 (c)(6), solicit public comment	06/30/22	*Complete*	No change	Complete.
Establish a 5 Year Operating Plan governing the full operational capability of the program.	09/30/22	*Complete*	Change	Complete
Produce a Report describing the initial full operational year of the Cyber Sense Program and will describe how it met the goals, measures, and metrics established in 2022	09/30/23	*On-Track*		

Narrative – FY 23 Q1

- In Q1 FY2023, CyTRICS prepared final reports on 3 systems (Tricon, TriconCX, and ION 8650) and shared them with DOE and their respective vendors (October). As of Q2 FY2023, CyTRICS continues testing on 1 large system (MACH3) and is preparing the final report for another system (RTAC 3530), both of which began testing in FY2022. Lastly, CyTRICS is starting to plan for 5 upcoming tests that are expected to complete in FY2023 (RTU 530, TRO 620, SAGE RTU, RTAC 3555, and GE turbine controller). It is anticipated that the Program may begin testing on another 2-3 systems, which will extend into FY2024, contingent upon the signing of new partner agreements.

- CyTRICS signed an agreement with GE Gas Power in Q2 of FY2023 and is exploring another agreement with GE Renewable Energy. CyTRICS is also pursuing agreements with OSISoft, Siemens, and Bloom Energy. Each agreement expands the number of participation manufacturers in the program and enables testing a broader number critical components in the energy sector. CyTRICS is also actively renewing agreements with Schneider Electric, Hitachi Energy, and Schweitzer Electrical Laboratories, which automatically expire after 2 years.

- The technical paper describing the methodology for sizing component testing is still slated for publication in Q2 FY2023, although with test planning on 5 new systems underway, this may slip into Q3 in order to collect data more data around the methodology's accuracy in predicting throughput and linking to resource levels.

Narrative – FY 23 Q1 cont…

- In addition, 4 of the 6 partner National Laboratories are now leading CyTRICS tests, representing a significant jump in the program's maturity and a significant scale-up in testing throughput. In FY2022, only 2 out of the 6 National Laboratories led CyTRICS tests. While partner National Laboratories often receive systems for testing directly from partner vendors, DOE CESER takes the lead in managing all vendor relationship.

- In Q1 FY2023, CESER completed the Energy Cyber Sense Implementation Plan and 5-Year Operating Plan. CESER is now expanding the program beyond the 8 requirements in the IIJA statute to meet four pillars of excellence: Understand criticality, Test and establish digital supply chain transparency, Aid in application of standards, norms, and best practices. And Improve technology and system designs (both legacy and new). This expanded vision of the program will enable CESER to execute more effectively on Congressional direction and assist the Energy Sector Industrial Base (ESIB) in enhancing the resilience of critical infrastructure. Over the next six months, CESER will be soliciting the input of strategic stakeholders across the ESIB to ensure implementation of Energy Cyber Sense is as successful as possible.

Narrative – FY 23 Q2

- In Q2 of FY2023, CyTRICS began wrapping up Phases 1 and 2 of testing on the Hitachi Energy (HE) MACH3 system, submitting SBOMs and HBOMs to the central data repository and providing a writeup of three novel vulnerabilities discovered by Oak Ridge National Laboratory (ORNL) to the manufacturer. Because of the size of this system, a 3rd Phase is planned on the MACH3 later in FY2023, which will involve targeted testing of capabilities perceived to be of significant potential impact if interdicted or sabotaged; discussions are underway with HE to scope Phase 3. The final report of the Schweitzer Engineering Laboratories (SEL) RTAC 3530 was nearly complete in Q2 and slated for sharing with the manufacturer in early Q3, which will kick off CyTRICS testing planning on the related RTAC 3555. Test planning on the HE RTU 530, HE TRO 620, Schneider Electric (SE) SAGE RTU, and General Electric (GE) turbine controller continued through Q2 as these manufacturers prepared to ship equipment for in early Q3. To this end, Lead Testing Laboratories began preliminary assessments of all four systems, while awaiting the arrival of physical hardware.

- CyTRICS kicked off collaborations with the DOE Solar Energy Technologies Office (SETO) and Wind Energy Technologies Office (WETO) in Q2 to evaluate critical emerging energy technologies. Hardware enumeration started on a common solar inverter while, while hardware enumeration on a common wind turbine controller will begin in Q3. The program is also actively exploring a strategic collaboration with the DOE Office of Nuclear Energy, which will likely lead to hardware enumeration of critical components in the nuclear subsector. These solar, wind, and nuclear engagements aim to expand the program situational awareness of critical components across energy subsectors.

Narrative – FY 23 Q2 cont…

- Future agreements are targeted with Honeywell and Westinghouse to support the expansion of the program into the nuclear subsector. With the combined existing and new CyTRICS engagements, the program continues to exceed the goal of 30% of critical component manufacturers formally engaged in CyTRICS testing in FY2023 Q2.

- Finally, efforts continued to expand the Energy Cyber Sense program beyond the four requirements in statute to serve as the umbrella effort for all of DOE CESER's supply chain security efforts. The first set of targeted stakeholders – the National Laboratories – engaged in significant strategic planning efforts to shape four pillars of excellence, frame the National Center of Excellence, identify other related efforts the program should align with, and develop capabilities that will enable significant scaling up of the program in the coming five years.

Data accuracy & reliability

- **Definition of criteria and processes are underway**

The cyber vulnerability testing work undertaken by the program represents the first known instance of a programmatic approach to cyber vulnerability testing and common mode failure analysis. (Testing capability exists in many labs, but as an hoc function and not a systematic approach.) Consequently, the Energy Cyber Sense Program/ CyTRICS has defined and implemented numerous unique program processes – e.g., a prioritization algorithm, a test operations manual, formats for results capture, a categorization of level of effort, etc. – to enable standardization of results and future scaling to third-party testing performers.

- **Baselining activities are underway**

The program has defined an initial field of inquiry – i.e., top 10 digital components in energy systems, top 20 manufacturers of digital components in energy systems, etc. – to establish preliminary baselines and goals. The initial definition was synthesized from a combination of market research data, self-reported data on market share, installed base by program participants, and subject matter expert judgements. These data will continue to be refined and validated as additional industry participants are added.