Agency Priority Goal | Action Plan | FY 2022, Q1 – Q4

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 Repeat the achievement statement from the goal statement on the previous slide		Key indicator(s) A "key performance indicator" measures progress toward a goal target	Quantify progress These values enable us (and you!) to calculate % complete for any type of target*			Frequency When is there new data?
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	*Late*	Change	Expected completion by 11-14-2022. Delay in strategic plan affected dependent products.
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 22 Q1 –Q2

- The Cyber Testing for Resilient Industrial Control Systems (CyTRICSTM) program achieved initial operating capability in FY2021 and began defining gating criteria for full operating capability for the program in Q1 of FY2022, with a goal of achieving full operating capability by the end of FY2022.

- Initial experience with test operations in FY2021 resulted in the first definition of standard criteria for sizing component testing (required because digital components vary widely in size and level of effort for testing) in Q1 of FY2022; this is a necessary step towards measuring program throughput.

- A major energy sector asset owner signed a CyTRICS participation agreement with DOE in Q1 of FY2022, brining the total of industry partners to 5; participation at the end of Q1 FY2022 now represents approximately 10% of total market share of critical components (overall goal is 30%)

- The Infrastructure Investment and Jobs Act (IIJA) became law in Q1 of FY2022 and directed DOE cyber vulnerability testing efforts under the new voluntary Energy Cyber Sense Program; adjustments to reflect the integration of CyTRICS under the Energy Cyber Sense program commenced in Q1 and will conclude at the end of Q2 of FY2022.

- The extended FY2022 Continuing Resolution will impact the program's ability to scale up testing throughput; unpredictability of funding is impeding participating Labs' ability to hire additional test performers and analysts.

Narrative – FY 22 Q2

- The Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program completed defining gating criteria for full operating capability for the program in Q2 of FY2022, with a goal of achieving full operating capability by the end of FY2022.

- CyTRICS pilot tested its standard criteria for sizing component testing (required because digital components vary widely in size and level of effort for testing) in Q2 of FY2022; this is a necessary step towards measuring program throughput. CyTRICS will publish a technical paper describing its unique sizing methodology in Q3.

- The 6 National Labs participating in CyTRICS completed a performance measurement baselining workshop in Q2; this is an interim step to completing APG measurement processes for the scheduled update at the end of Q4.

- The Infrastructure Investment and Jobs Act (IIJA) became law in Q1 of FY2022 and directed DOE cyber vulnerability testing efforts under the new voluntary Energy Cyber Sense Program. In Q2, CESER drafted a high-level Energy Cyber Sense Strategy showing how it will integrate CyTRICS and related cyber supply chain initiatives to meet congressional direction. The extended FY2022 Continuing Resolution impacted timely completion of this milestone. Completion will occur in June.

Narrative – FY 22 Q3

- The Cyber Testing for Resilient Industrial Control Systems (CyTRICSTM) program will finalize a new testing agreement with GE Research in Q4. This will support meeting the goal of signing up manufacturers who represent 30% of critical components by the end of FY2022.

- CyTRICS pilot tested its standard criteria for sizing component testing (required because digital components vary widely in size and level of effort for testing) in Q2 of FY2022; this is a necessary step towards measuring program throughput and linking it to resource levels. CyTRICS will publish a technical paper describing its unique sizing methodology in Q4.

- The 6 National Labs participating in CyTRICS completed a performance measurement baselining workshop in Q2; this is an interim step to completing APG measurement processes for the scheduled update at the end of Q4.

- The Infrastructure Investment and Jobs Act (IIJA) became law in Q1 of FY2022 and directed DOE cyber vulnerability testing efforts under the new voluntary Energy Cyber Sense Program. CESER drafted a high-level Energy Cyber Sense Strategy showing how it will integrate CyTRICS and related cyber supply chain initiatives to meet congressional direction, and a draft approach to testing, per direction in the statute. These are both complete and being readied for public release.

Narrative – FY 22 Q4

- In 2022, CyTRICS initiated testing on 11 products. Five tests were completed, Five are pending the final report completion, and one is proceeding into 2023. Systems tested cover energy subsectors including Electric, Nuclear, Oil and Natural Gas, and Renewable Energy.

- The Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program surpassed its 2022 goal to expand participating manufacturers to cover 15% of the market share of critical components. Based on market analysis, CyTRICS achieved participating vendors representing 34%. CyTRICS will finalize a new testing agreement with GE Renewable Energy in Q1, 2023. This will support meeting the goal of signing up manufacturers who represent 30% of critical components by the end of FY2023.

- CyTRICS pilot tested its standard criteria for sizing component testing (required because digital components vary widely in size and level of effort for testing) in Q2 of FY2022; this is a necessary step towards measuring program throughput and linking it to resource levels. CESER developed a Standard Operating Procedure (SOP) to allow the methodology to be validated within the project and postponed plans to publish a technical paper describing its unique sizing methodology until Q2 of 2023, when the methodology has been tested.

- The Infrastructure Investment and Jobs Act (IIJA) became law in Q1 of FY2022 and directed DOE cyber vulnerability testing efforts under the new voluntary Energy Cyber Sense Program. CESER drafted Energy Cyber Sense Strategy showing how it will integrate CyTRICS and related cyber supply chain initiatives to meet congressional direction, and a draft approach to testing, per direction in the statute. CESER is finalizing the implementation plan, 5-year operating plan, and performance reporting for Q1, FY23.

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.