U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

BETO Bioenergy Cybersecurity Workshop

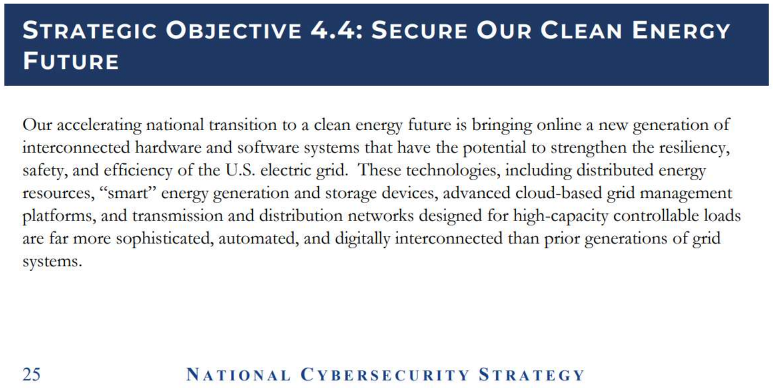
Jessica Perry, CESER
Cyber RD&D Technical Program Manager

September 11, 2023

Federal Priorities and Perspectives

NATIONAL CYBERSECURITY STRATEGY

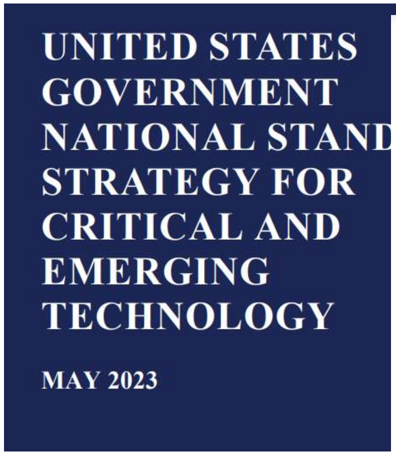
MARCH 2023



STRATEGIC OBJECTIVE 4.4: SECURE OUR CLEAN ENERGY FUTURE

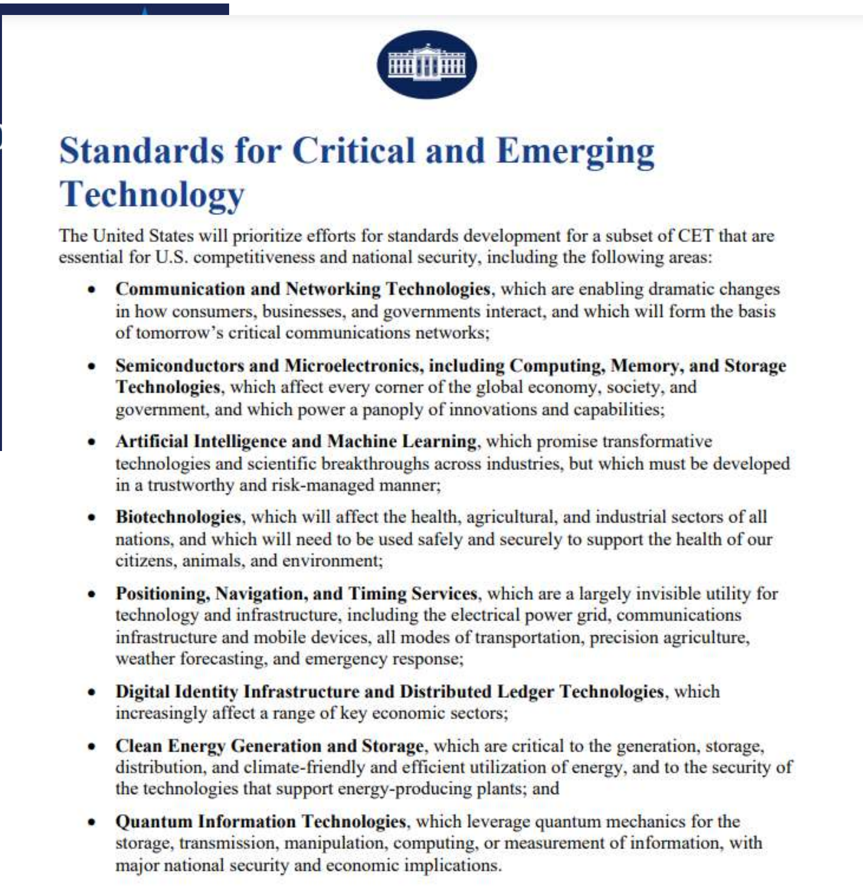
Our accelerating national transition to a clean energy future is bringing online a new generation of interconnected hardware and software systems that have the potential to strengthen the resiliency, safety, and efficiency of the U.S. electric grid. These technologies, including distributed energy resources, "smart" energy generation and storage devices, advanced cloud-based grid management platforms, and transmission and distribution networks designed for high-capacity controllable loads are far more sophisticated, automated, and digitally interconnected than prior generations of grid systems.

25 NATIONAL CYBERSECURITY STRATEGY



UNITED STATES GOVERNMENT NATIONAL STAND STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY

MAY 2023



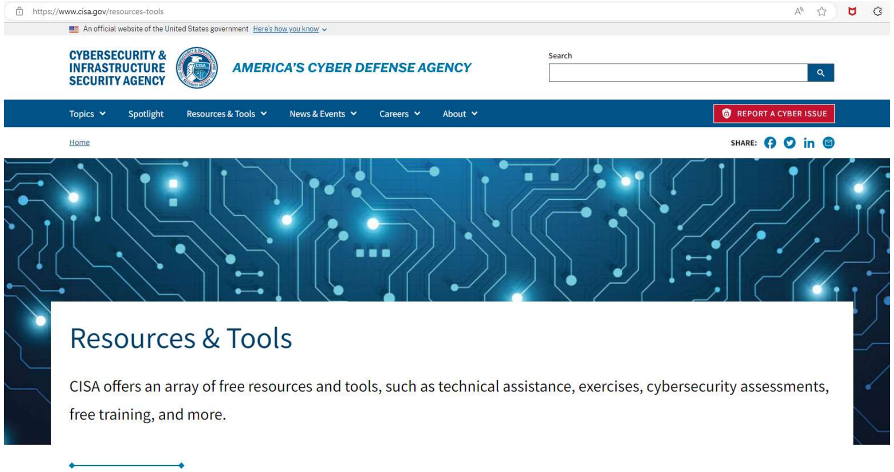
Standards for Critical and Emerging Technology

The United States will prioritize efforts for standards development for a subset of CET that are essential for U.S. competitiveness and national security, including the following areas:

- **Communication and Networking Technologies**, which are enabling dramatic changes in how consumers, businesses, and governments interact, and which will form the basis of tomorrow's critical communications networks;
- **Semiconductors and Microelectronics, including Computing, Memory, and Storage Technologies**, which affect every corner of the global economy, society, and government, and which power a panoply of innovations and capabilities;
- **Artificial Intelligence and Machine Learning**, which promise transformative technologies and scientific breakthroughs across industries, but which must be developed in a trustworthy and risk-managed manner;
- **Biotechnologies**, which will affect the health, agricultural, and industrial sectors of all nations, and which will need to be used safely and securely to support the health of our citizens, animals, and environment;
- **Positioning, Navigation, and Timing Services**, which are a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response;
- **Digital Identity Infrastructure and Distributed Ledger Technologies**, which increasingly affect a range of key economic sectors;
- **Clean Energy Generation and Storage**, which are critical to the generation, storage, distribution, and climate-friendly and efficient utilization of energy, and to the security of the technologies that support energy-producing plants; and
- **Quantum Information Technologies**, which leverage quantum mechanics for the storage, transmission, manipulation, computing, or measurement of information, with major national security and economic implications.

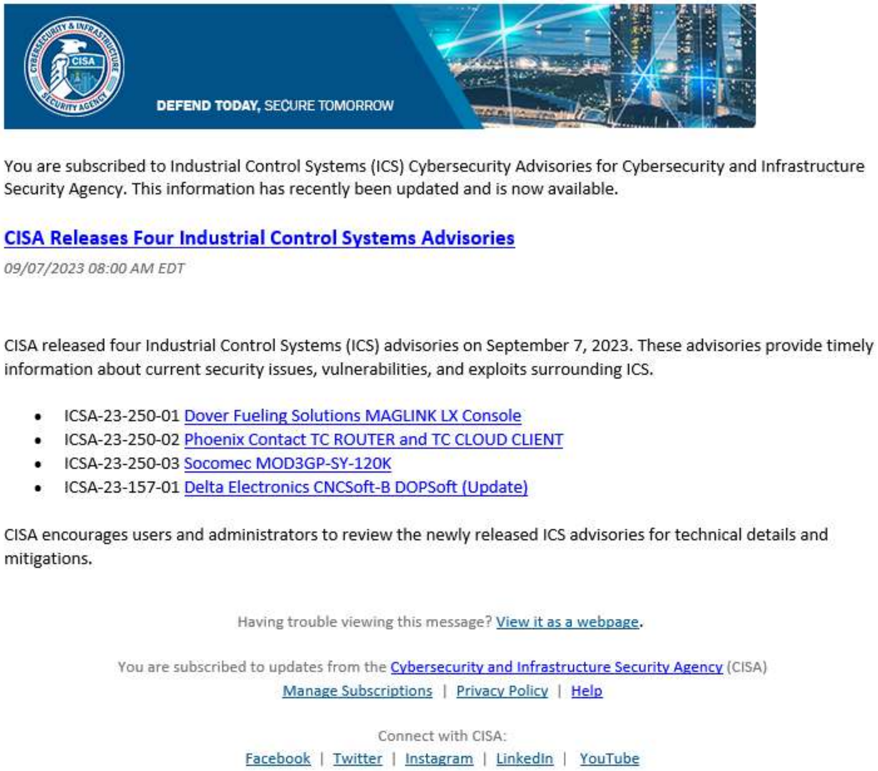
CISA

- CISA Cybersecurity Strategic Plan | CISA


https://www.cisa.gov/resources-tools
An official website of the United States government Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home
SHARE:

Resources & Tools

CISA offers an array of free resources and tools, such as technical assistance, exercises, cybersecurity assessments, free training, and more.



You are subscribed to Industrial Control Systems (ICS) Cybersecurity Advisories for Cybersecurity and Infrastructure Security Agency. This information has recently been updated and is now available.

CISA Releases Four Industrial Control Systems Advisories

09/07/2023 08:00 AM EDT

CISA released four Industrial Control Systems (ICS) advisories on September 7, 2023. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

- ICSA-23-250-01 Dover Fueling Solutions MAGLINK LX Console
- ICSA-23-250-02 Phoenix Contact TC ROUTER and TC CLOUD CLIENT
- ICSA-23-250-03 Socomec MOD3GP-SY-120K
- ICSA-23-157-01 Delta Electronics CNCSoft-B DOPSoft (Update)

CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

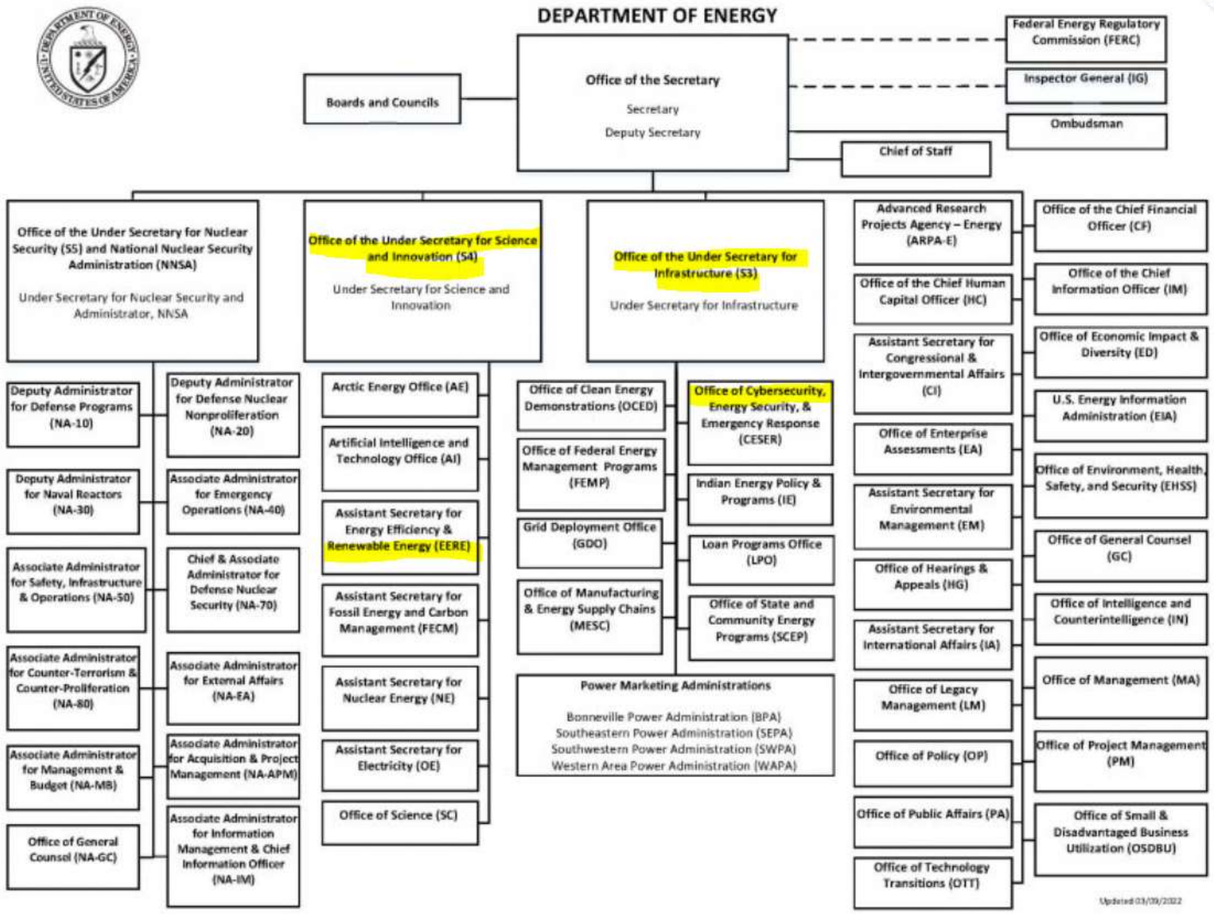
Having trouble viewing this message? View it as a webpage.

You are subscribed to updates from the Cybersecurity and Infrastructure Security Agency (CISA)
Manage Subscriptions | Privacy Policy | Help

Connect with CISA:
Facebook | Twitter | Instagram | LinkedIn | YouTube

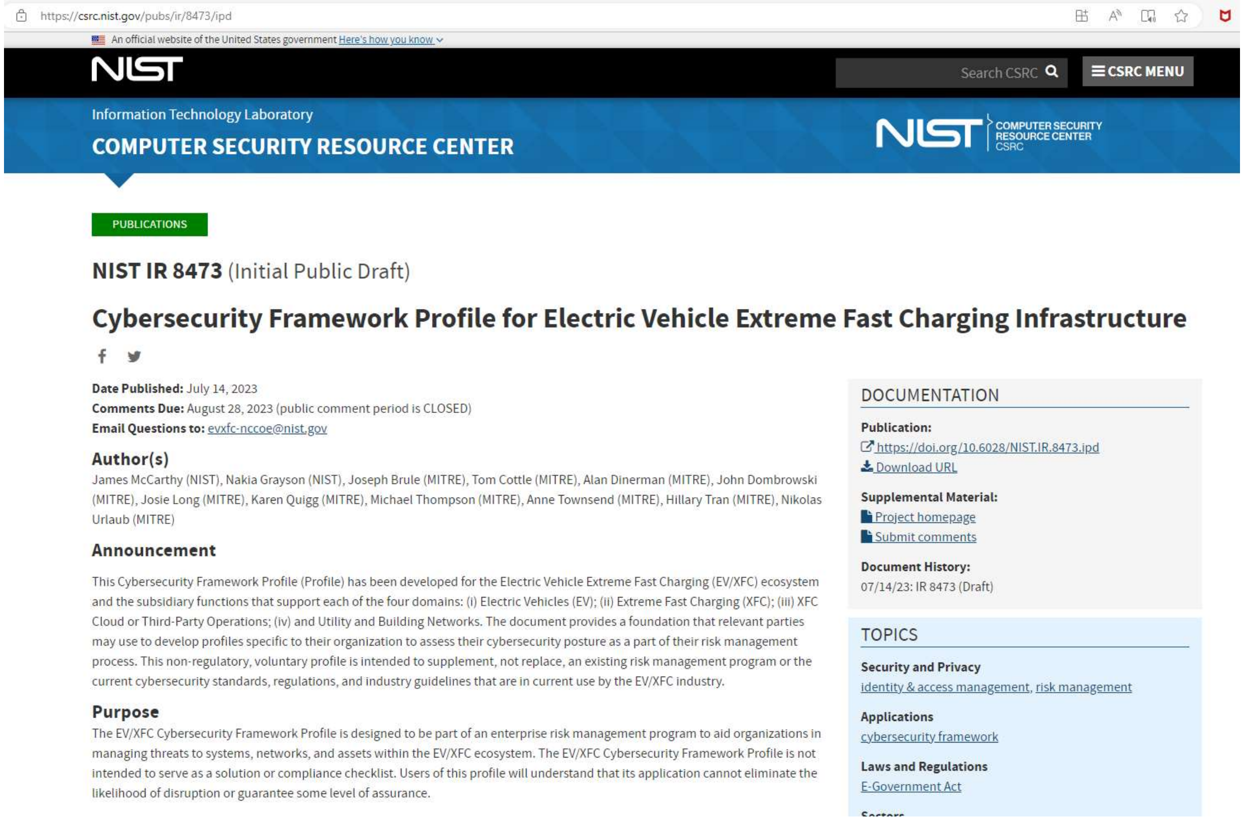
DOE

- Program Office R&D
- Cyber R&D Coordination
- GMI


DEPARTMENT OF ENERGY
Office of the Secretary
Secretary
Deputy Secretary
Boards and Councils
Federal Energy Regulatory Commission (FERC)
Inspector General (IG)
Ombudsman
Chief of Staff
Office of the Under Secretary for Nuclear Security (S5) and National Nuclear Security Administration (NNSA)
Under Secretary for Nuclear Security and Administrator, NNSA
Office of the Under Secretary for Science and Innovation (S4)
Under Secretary for Science and Innovation
Office of the Under Secretary for Infrastructure (S3)
Under Secretary for Infrastructure
Advanced Research Projects Agency – Energy (ARPA-E)
Office of the Chief Human Capital Officer (HC)
Assistant Secretary for Congressional & Intergovernmental Affairs (CI)
Office of Enterprise Assessments (EA)
Assistant Secretary for Environmental Management (EM)
Office of Hearings & Appeals (HG)
Assistant Secretary for International Affairs (IA)
Office of Legacy Management (LM)
Office of Policy (OP)
Office of Public Affairs (PA)
Office of Technology Transitions (OTT)
Office of the Chief Financial Officer (CF)
Office of the Chief Information Officer (IM)
Office of Economic Impact & Diversity (ED)
U.S. Energy Information Administration (EIA)
Office of Environment, Health, Safety, and Security (EHSS)
Office of General Counsel (GC)
Office of Intelligence and Counterintelligence (IN)
Office of Management (MA)
Office of Project Management (PM)
Office of Small & Disadvantaged Business Utilization (OSDBU)
Deputy Administrator for Defense Programs (NA-10)
Deputy Administrator for Naval Reactors (NA-30)
Associate Administrator for Safety, Infrastructure & Operations (NA-50)
Associate Administrator for Counter-Terrorism & Counter-Proliferation (NA-80)
Associate Administrator for Management & Budget (NA-MB)
Office of General Counsel (NA-GC)
Deputy Administrator for Defense Nuclear Nonproliferation (NA-20)
Associate Administrator for Emergency Operations (NA-40)
Chief & Associate Administrator for Defense Nuclear Security (NA-70)
Associate Administrator for External Affairs (NA-EA)
Associate Administrator for Acquisition & Project Management (NA-APM)
Associate Administrator for Information Management & Chief Information Officer (NA-IM)
Arctic Energy Office (AE)
Artificial Intelligence and Technology Office (AI)
Assistant Secretary for Energy Efficiency & Renewable Energy (EERE)
Assistant Secretary for Fossil Energy and Carbon Management (FECM)
Assistant Secretary for Nuclear Energy (NE)
Assistant Secretary for Electricity (OE)
Office of Science (SC)
Office of Clean Energy Demonstrations (OCED)
Office of Federal Energy Management Programs (FEMP)
Grid Deployment Office (GDO)
Office of Manufacturing & Energy Supply Chains (MESC)
Office of Cybersecurity, Energy Security, & Emergency Response (CESER)
Indian Energy Policy & Programs (IE)
Loan Programs Office (LPO)
Office of State and Community Energy Programs (SCEP)
Power Marketing Administrations
Bonneville Power Administration (BPA)
Southeastern Power Administration (SEPA)
Southwestern Power Administration (SWPA)
Western Area Power Administration (WAPA)
Updated 03/09/2022

DOE Organization Chart - Updated March 2022

DOE Program Offices co-fund projects


https://csrc.nist.gov/pubs/ir/8473/ipd
An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PUBLICATIONS

NIST IR 8473 (Initial Public Draft)

Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure

Date Published: July 14, 2023
Comments Due: August 28, 2023 (public comment period is CLOSED)
Email Questions to: evxfc-nccoe@nist.gov

Author(s)

James McCarthy (NIST), Nakia Grayson (NIST), Joseph Brule (MITRE), Tom Cottle (MITRE), Alan Dinerman (MITRE), John Dombrowski (MITRE), Josie Long (MITRE), Karen Quigg (MITRE), Michael Thompson (MITRE), Anne Townsend (MITRE), Hillary Tran (MITRE), Nikolas Urlaub (MITRE)

Announcement

This Cybersecurity Framework Profile (Profile) has been developed for the Electric Vehicle Extreme Fast Charging (EV/XFC) ecosystem and the subsidiary functions that support each of the four domains: (i) Electric Vehicles (EV); (ii) Extreme Fast Charging (XFC); (iii) XFC Cloud or Third-Party Operations; (iv) and Utility and Building Networks. The document provides a foundation that relevant parties may use to develop profiles specific to their organization to assess their cybersecurity posture as a part of their risk management process. This non-regulatory, voluntary profile is intended to supplement, not replace, an existing risk management program or the current cybersecurity standards, regulations, and industry guidelines that are in current use by the EV/XFC industry.

Purpose

The EV/XFC Cybersecurity Framework Profile is designed to be part of an enterprise risk management program to aid organizations in managing threats to systems, networks, and assets within the EV/XFC ecosystem. The EV/XFC Cybersecurity Framework Profile is not intended to serve as a solution or compliance checklist. Users of this profile will understand that its application cannot eliminate the likelihood of disruption or guarantee some level of assurance.

DOCUMENTATION

Publication:
https://doi.org/10.6028/NIST.IR.8473.ipd
Download URL

Supplemental Material:
Project homepage
Submit comments

Document History:
07/14/23: IR 8473 (Draft)

TOPICS

Security and Privacy
identity & access management, risk management

Applications
cybersecurity framework

Laws and Regulations
E-Government Act

Sectors

Grid Modernization Initiative (GMI)

- GMLC
- Grid Modernization Summit Feb 6-8, 2024

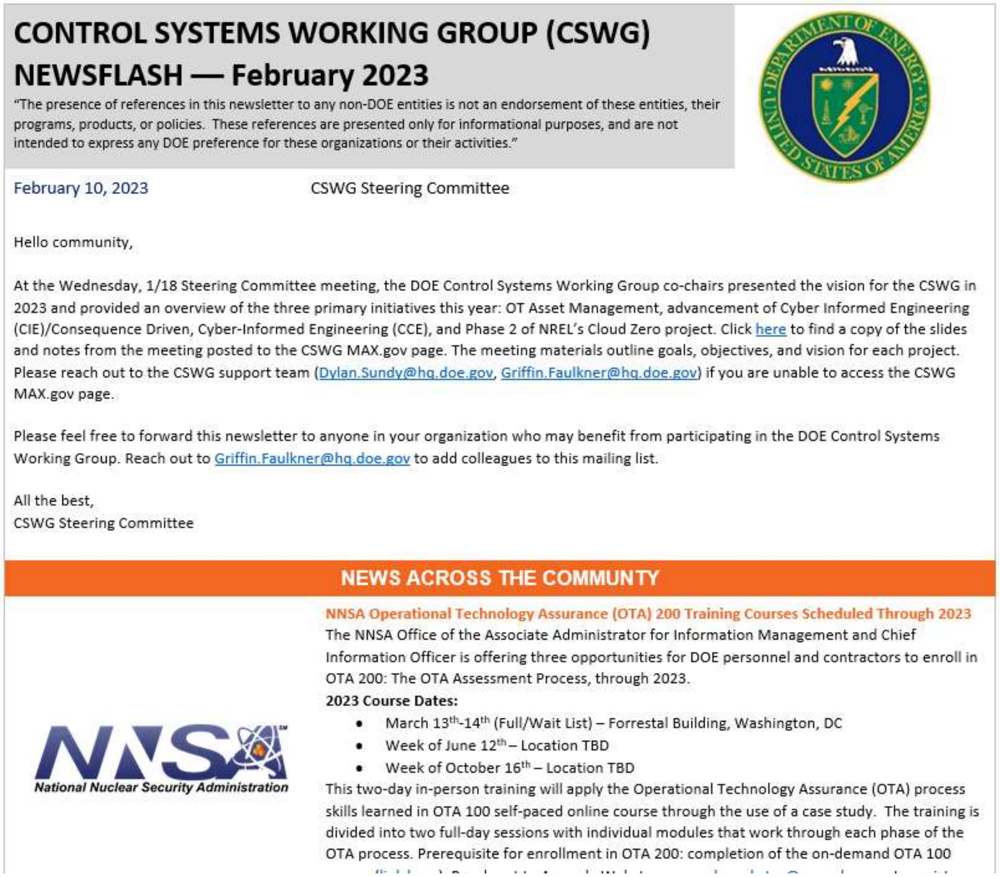
- 2023 Lab call
  - DOE Invests $39 Million to Support a 21st Century Electric Grid | Department of Energy

  - **Aligning Climate Analysis for Power Systems (ALCAPS) and Climate Resilient Equitable Resource Planning (CRERP).** This project led by NREL will take multiple approaches to integrate acute and chronic effects of climate change across a suite of energy sector planning and risk management tools. This project team will do this by connecting, expanding, and enhancing established methodologies such as generative machine learning and supply modeling in order to study possible stresses on the energy system caused by climate change. This includes efforts to better understand of the impacts of extreme weather on available wind, solar and hydropower resources as well as energy demand, implications for siting of renewable energy and transmission, and potential climate-driven changes in water availability for energy related needs including thermal cooling.

DOE’s Control Systems Working Group (CSWG)

The Department of Energy’s Control Systems Working Group is a platform for DOE’s Industrial Control Systems (ICS) and Operational Technology (OT) system owners, researchers, and industry experts to convene and address challenges and pain points associated with reducing cyber risk in ICS/OT environments.

It is co-led by the DOE Office of the Chief Information Officer (OCIO) and National Nuclear Security Administration (NNSA) Office of the Chief Information Officer. The CSWG’s priorities are driven by the priorities of DOE’s ICS/OT system owners and operators.



CONTROL SYSTEMS WORKING GROUP (CSWG)

NEWSFLASH — February 2023

“The presence of references in this newsletter to any non-DOE entities is not an endorsement of these entities, their programs, products, or policies. These references are presented only for informational purposes, and are not intended to express any DOE preference for these organizations or their activities.”

February 10, 2023 CSWG Steering Committee

Hello community,

At the Wednesday, 1/18 Steering Committee meeting, the DOE Control Systems Working Group co-chairs presented the vision for the CSWG in 2023 and provided an overview of the three primary initiatives this year: OT Asset Management, advancement of Cyber Informed Engineering (CIE)/Consequence Driven, Cyber-Informed Engineering (CCE), and Phase 2 of NREL’s Cloud Zero project. Click here to find a copy of the slides and notes from the meeting posted to the CSWG MAX.gov page. The meeting materials outline goals, objectives, and vision for each project. Please reach out to the CSWG support team (Dylan.Sundy@hq.doe.gov, Griffin.Faulkner@hq.doe.gov) if you are unable to access the CSWG MAX.gov page.

Please feel free to forward this newsletter to anyone in your organization who may benefit from participating in the DOE Control Systems Working Group. Reach out to Griffin.Faulkner@hq.doe.gov to add colleagues to this mailing list.

All the best,
CSWG Steering Committee

NEWS ACROSS THE COMMUNTY

NNSA Operational Technology Assurance (OTA) 200 Training Courses Scheduled Through 2023

The NNSA Office of the Associate Administrator for Information Management and Chief Information Officer is offering three opportunities for DOE personnel and contractors to enroll in OTA 200: The OTA Assessment Process, through 2023.

2023 Course Dates:

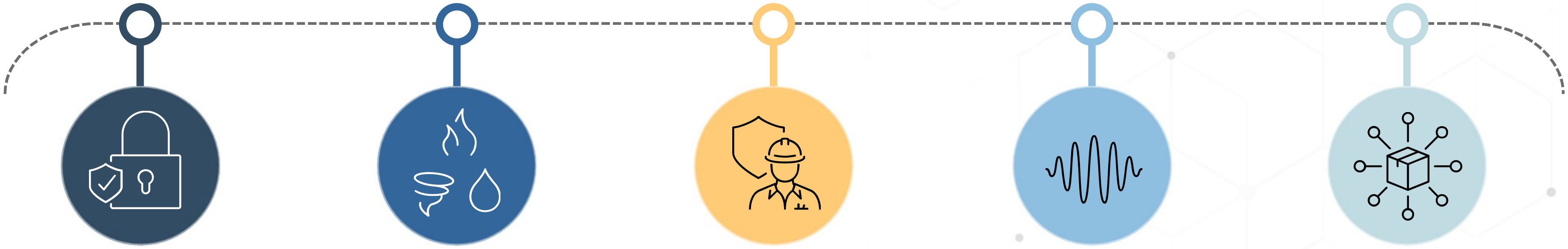
- March 13th-14th (Full/Wait List) – Forrestal Building, Washington, DC
- Week of June 12th – Location TBD
- Week of October 16th – Location TBD

This two-day in-person training will apply the Operational Technology Assurance (OTA) process skills learned in OTA 100 self-paced online course through the use of a case study. The training is divided into two full-day sessions with individual modules that work through each phase of the OTA process. Prerequisite for enrollment in OTA 200: completion of the on-demand OTA 100

CESER Mission

Strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions.

Evolving Threats to Energy Infrastructure



Cyber Threats

Climate Risks

Physical Threats

EMP | GMD

Supply Chain

Risk Management Tools and Technologies (RMT)

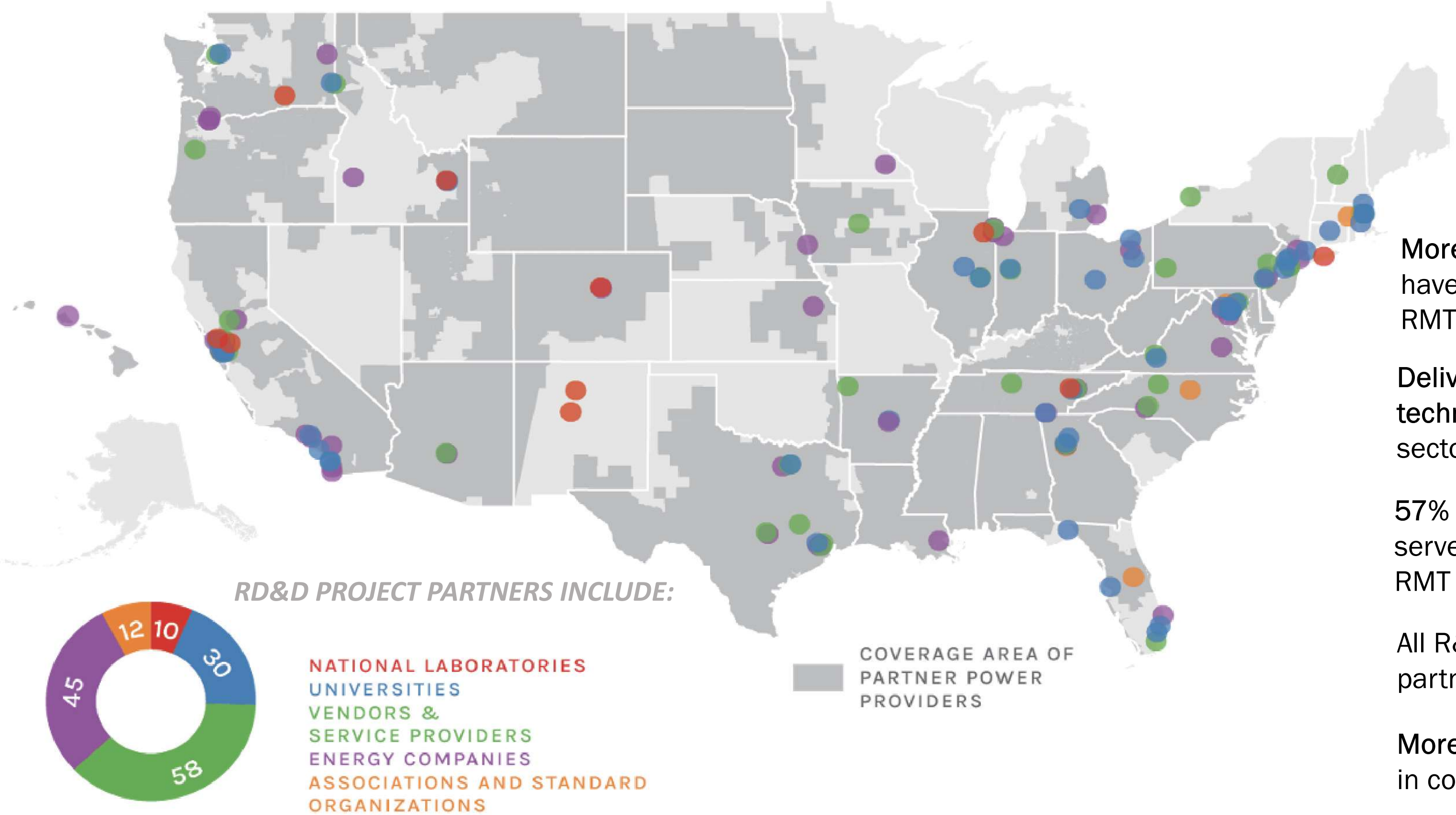
RMT leads research, development and demonstration of tools, technologies, and techniques that help manage cyber and physical risks to critical energy systems.

The RMT division is organized by 2 focus areas:

- All-hazards Tools and Technologies address natural and human made physical risks to energy systems such as extreme weather, wildfires, climate change, seismic activity, electromagnetic pulse (EMP) and geomagnetic disturbances (GMD)
- Cyber Tools and Technologies enable innovative protection, detection, and response solutions to address energy delivery systems.

QKD Transceiver

RMT Cyber Research, Development, and Deployment


RD&D PROJECT PARTNERS INCLUDE:
12
10
30
58
45
NATIONAL LABORATORIES
UNIVERSITIES
VENDORS & SERVICE PROVIDERS
ENERGY COMPANIES
ASSOCIATIONS AND STANDARD ORGANIZATIONS
COVERAGE AREA OF PARTNER POWER PROVIDERS

More than 1,500 utilities in all 50 states have purchased products developed under RMT research

Delivered over 90 products, tools, and technologies since 2010 to reduce energy sector cyber risk

57% of U.S. electricity customers are served by power providers participating in RMT R&D

All R&D projects included an energy sector partner to drive **real-world solutions**

More than 155 partners have participated in competitively funded projects

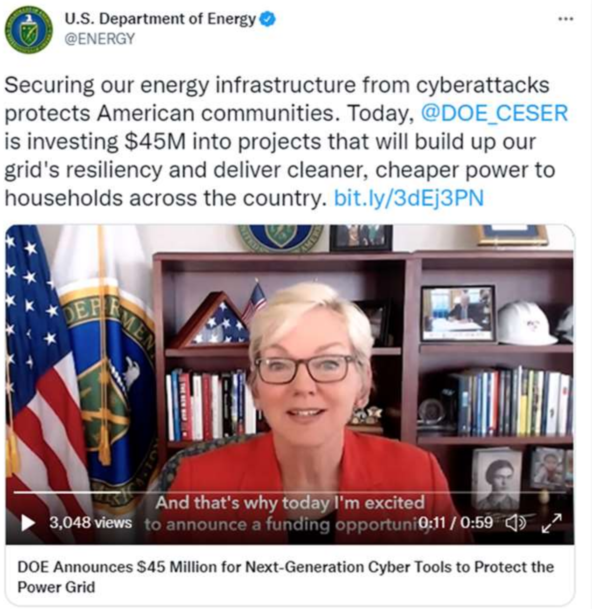
Active RMT Funding Opportunity Announcements

FOA 2503 - $12M University-Based Cybersecurity Centers

- Objective: To establish academic collaboration centers distributed regionally across the country.
  - Innovate and transition capabilities that reduce the risk of power disruption resulting from a cyber-incident for energy delivery systems.
  - Develop and build a system of cybersecurity education for the energy sector.

FOA 2500 - $45M CYBER RD&D

- Objective: To advance cybersecurity tools and technologies specifically designed to reduce cyber risks to energy delivery infrastructure.



U.S. Department of Energy
@ENERGY

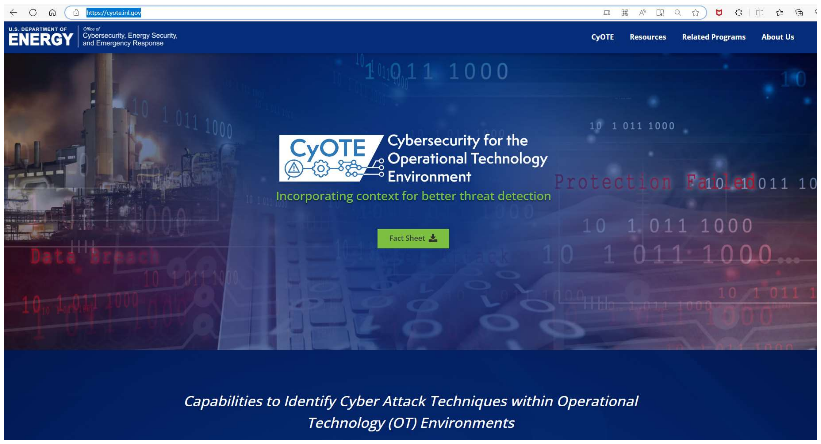
Securing our energy infrastructure from cyberattacks protects American communities. Today, @DOE_CESER is investing $45M into projects that will build up our grid's resiliency and deliver cleaner, cheaper power to households across the country. bit.ly/3dEj3PN

And that's why today I'm excited
to announce a funding opportuni

DOE Announces $45 Million for Next-Generation Cyber Tools to Protect the Power Grid

Sample of RMT RD&D

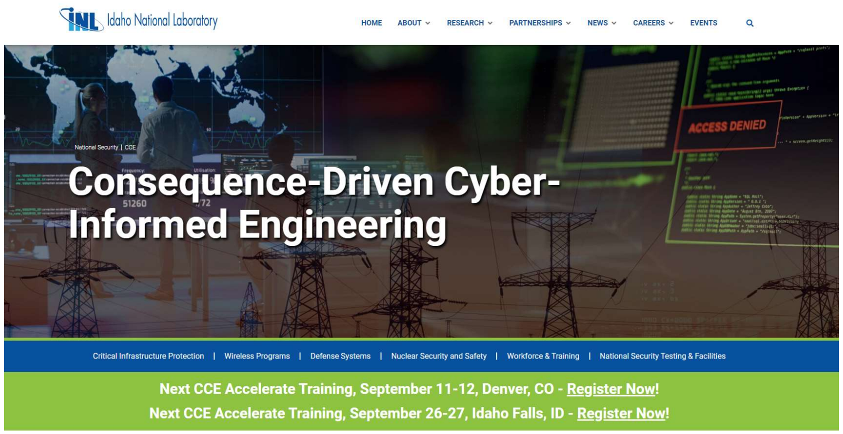
- DER
- EVSE
  - Includes cyber technology for AFV
- Securing infrastructure : OT, Energy Supply Chain, etc
- Secure by Design: Cyber-Informed Engineering (CIE)


https://cyote.inl.gov
U.S. DEPARTMENT OF ENERGY
Office of Cybersecurity, Energy Security, and Emergency Response
CyOTE
Resources
Related Programs
About Us
Fact Sheet

CyOTE Cybersecurity for the Operational Technology Environment

Incorporating context for better threat detection

Capabilities to Identify Cyber Attack Techniques within Operational Technology (OT) Environments


INL Idaho National Laboratory
HOME
ABOUT
RESEARCH
PARTNERSHIPS
NEWS
CAREERS
EVENTS
National Security | CCE
Critical Infrastructure Protection | Wireless Programs | Defense Systems | Nuclear Security and Safety | Workforce & Training | National Security Testing & Facilities

Consequence-Driven Cyber-Informed Engineering

Next CCE Accelerate Training, September 11-12, Denver, CO - Register Now!

Next CCE Accelerate Training, September 26-27, Idaho Falls, ID - Register Now!

$14M University-Based R&D of Scalable Cyber-Physical Solutions

FIU FLORIDA INTERNATIONAL UNIVERSITY

The project will develop artificial intelligence (AI)-based detection tools and design effective cyber threat mitigation strategies using these technologies. (Award Amount: $2,000,000)

IOWA STATE UNIVERSITY

The project will enable defense-in-depth security and resilience for cyber-physical systems using AI-integrated, attack-resilient, and proactive system technologies and solutions. (Award Amount: $2,000,000)

NEW YORK UNIVERSITY

The project will develop a program called Tracking Real-time Anomalies in Power Systems (TRAPS) to detect and localize anomalies in power grid cyber-physical systems. (Award Amount: $1,939,416)

TEES TEXAS A&M ENGINEERING EXPERIMENT STATION

The project will leverage AI and machine learning to develop techniques and scalable prototypes for intrusion response against advanced cyber-physical threats to power systems. (Award Amount: $1,997,921)

UIC UNIVERSITY OF ILLINOIS CHICAGO

The project will develop a resilient, next-generation solid-state power substation, integrating cybersecurity considerations to improve adoptability. (Award Amount: $2,000,000)

VT VIRGINIA TECH™

The project will create a program called Cyber REsilience of SubsTations (CREST), a two-part system to detect and mitigate cyber incidents while maintaining secure communication and critical functions. (Award Amount: $1,997,864)

Questions?

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response