

# ENERGY MODERNIZATION CYBERSECURITY IMPLEMENTATION PLAN

DECEMBER 2024



THE WHITE HOUSE  
WASHINGTON



# Table of Contents

Introduction .....	4
Overview .....	4
A Changing Grid .....	4
Facing Evolving Threats .....	5
Linchpin Technologies .....	5
Implementation Plan Reading Guide .....	7
Section A: Cross-Cutting Issues .....	8
Goal: Enhance operational collaboration between government and energy sector partners .....	8
Goal: Create communities of practice able to foster strategic unity, shared goals, and critical information flows .....	10
Goal: Link digital energy infrastructure standards requirements to cross-cutting standards agenda .....	12
Goal: Get “ahead of the curve” on cybersecurity practices for key currently- or soon-deploying technologies .....	13
Goal: Develop a better understanding of potential cybersecurity risks with the next generation of energy technology .....	14
Goal: Strengthen energy technology cybersecurity R&D community of practice capable of identifying priority R&D requirements .....	15
Goal: Build cybersecurity considerations into the foundations of energy modernization, while ensuring it is flexible enough to accommodate not-yet-extant cybersecurity practices as they develop .....	16
Goal: Develop a better understanding of potential cybersecurity risks with the next generation of energy technology .....	17
Goal: Identify evolving landscape of energy system products bought and installed in the United States .....	19
Goal: Develop a modern energy cybersecurity workforce .....	20
Section B: Batteries & Battery Management Systems .....	21
Goal: Create community of practice able to foster strategic unity, shared goals, and critical information flows .....	21
Goal: Enhance operational collaboration between government and energy sector partners .....	22
Section C: Inverters Controls & Power Conversion Equipment .....	23
Goal: Enhance operational collaboration between government and energy sector partners .....	23
Goal: Develop strategic cyber interconnection plan to enable guidelines to be pushed more regularly to the process of connection to the grid .....	24



Goal: Get “ahead of the curve” on cybersecurity practices for key currently- or soon-deploying technologies .....	25
<b>Section D: Distributed Control Systems .....</b>	<b>26</b>
Goal: Harmonize integration and management of DERs through common data standards.....	26
Goal: Build cybersecurity considerations into the foundations of distributed control systems rollout while ensuring they are flexible enough to accommodate not-yet-extant standards as they develop.....	27
<b>Section E: Building Energy Management Systems .....</b>	<b>28</b>
Goal: Get “ahead of the curve” on cybersecurity practices for key currently- or soon-deploying technologies .....	28
Goal: Diagnose building management system supply chain risk from a cybersecurity perspective and adopt appropriate mitigations .....	29
<b>Section F: Electric Vehicles (EVs) &amp; Electric Vehicle Supply Equipment (EVSE) .....</b>	<b>30</b>
Goal: Create communities of practice able to foster strategic unity, shared goals, and critical information flows.....	30
Goal: Accelerate the development of cybersecurity-focused technical standards and related guidance, including energy sector CPGs and NIST Privacy Framework profile for EV/EVSE .....	32
Goal: Drive international adoption of secure modern energy technologies, including EV/EVSE .....	33
Goal: Ensure EVSE platforms are flexible enough to accommodate not-yet-extant standards as they develop.....	34
Goal: Support agency procurement of secure electric vehicle-related infrastructure .....	36
Goal: Develop an EV charging cybersecurity workforce .....	37
Goal: Enable cyber defenders and managers to better understand systemic risks presented by EVSE integrations and identify opportunities for mitigation .....	38



# Introduction

## Overview

America's energy landscape is modernizing as it becomes increasingly digitized. New internet-connected technologies enhance the efficiency, safety, and resiliency of the grid. These energy technologies, along with the systems that manufacture and operate them, benefit from the convergence of network-based information technology (IT) and operational technology (OT) systems – systems that manage physical processes and control of infrastructure. This convergence offers a variety of benefits, from reducing fuel costs and improving asset reliability to lessening the environmental impact of energy generation. But it also comes with risks that must be mitigated to realize a truly 21<sup>st</sup> Century vision of our power infrastructure.

Securing the American energy sector requires coordinated action across the United States Government and American society. The Energy Modernization Cybersecurity Implementation Plan (EMCIP) is a roadmap for this effort. While it does not capture all Federal cybersecurity activities related to the energy sector, the EMCIP outlines 32 high-impact initiatives requiring executive visibility and interagency coordination that the Federal government will carry out to achieve a more secure energy ecosystem. Each initiative is assigned to a Responsible Agency with a specific timeline for completion. Any Federal activities identified in this plan beyond those already reflected in the President's Budget will be subject to relevant budgetary processes.

The United States Government will only succeed in implementing this Plan through close collaboration with the private sector; civil society; state, local, Tribal, and territorial (SLTT) governments; international partners; and Congress. Federal agencies will collaborate with interested stakeholders to implement the Plan and build new partnerships where possible.

## A Changing Grid

The electric grid is undergoing a significant, rapid transformation which is redefining how the electric system needs to be designed, built, and operated. The deployment of variable generation, primarily wind and solar, is leading this transformation along with conventional generation retirements. Transmission grids are moving from the physics of large-spinning generation to power systems incorporating inverter-based resources, requiring fundamentally different designs and security paradigms.

Additionally, battery energy storage systems are beginning to be extensively deployed. This is in contrast to nearly the entire history of the electric grid, where pumped-storage hydroelectricity was the primary means of energy storage.

While much of this transformation is occurring on the transmission and sub-transmission systems, significant change is also happening at the grid edge with home and business owners installing distributed energy resources (DER) within the distribution system and behind the meter. DER deployment is expected to grow from approximately 90 gigawatts (GW) in 2024 to



approximately 380 GW by 2025.<sup>1</sup> Nearly half of DER today are solar photovoltaic (PV) systems, with millions of PV arrays atop homes across the country.

At the same time, the rapid, multi-party proliferation of these technologies also has the potential to introduce new cybersecurity risks to the energy ecosystem. Absent timely intervention, the electricity sector risks “locking in” these potential vulnerabilities and imperiling the security and reliability of the electric power system and the long-term viability of a robust national energy sector.

## Facing Evolving Threats

In the past decade, the energy sector’s vulnerability to remote cyber threats has increased as energy companies upgrade or expose OT to the Internet to address challenges associated with maintaining geographically complex systems. While Internet-accessible systems reduce cost and improve operational efficiencies, many widely-deployed legacy technologies are not designed to operate securely over the Internet.

This transformation presents emerging cybersecurity challenges for the reliability of the electric power grid. A key challenge is that utilities may not own, and often do not directly operate, the technologies and systems that are being connected. Historically, utilities were the primary entity responsible for the security and reliability of the electric power grid. As new technologies connect to the grid, new industries will need to bear responsibility for securing the resources they manufacture, deploy, maintain, and operate. Because many new market entrants have not been part of the established processes for oversight, operation, and maintenance of the power grid, their roles and responsibilities need to be established regarding electric power reliability and security requirements. In addition to grid transformation, the rapid evolution of ransomware threats; convergence of IT and OT systems; increased use of cloud-based communication and control systems; and expanding automation also create cybersecurity challenges.

## Linchpin Technologies

The United States Government is committed to ensuring the digital ecosystem is prepared for current and future challenges. Additional focus will be placed on five cyber-enabled technologies key to near-term energy modernization:

**Batteries & Battery Management Systems.** Batteries are poised to be foundational engines of the next generation of energy systems. They are enabling utility-scale storage of solar energy for nighttime dispatch; strengthening resilience and flexibility for commercial and residential owners of on-site battery packs; and enabling more affordable transportation from buses to cars to e-bikes. With properly architected and secured software, both firmware and cloud-based, batteries big and small promise an ambitious energy future that is less constrained by the time or geography of electricity generation.

---

<sup>1</sup> "The next five years will see massive distributed energy resource growth," *Wood Mackenzie*, <https://www.woodmac.com/news/editorial/der-growth-united-states/>.



**Inverter Controls & Power Conversion Equipment.** Inverter controls and power conversion equipment serve a simple function with profound import: converting power from direct current to alternating current, and vice versa. This process underpins every connection between the electrical grid and distributed energy resources, such as solar panels, batteries, wind turbines, or hydrogen electrolyzers. Modern smart inverters are equipped with advanced computing and networking capabilities. When paired with robust cybersecurity, these inverters support more sophisticated grid services, while promoting greater resilience and lower operating costs across diverse energy assets.

**Distributed Control Systems.** Industry continues to transform electricity generation, transmission, distribution, and storage assets into a more diverse, diffuse, and digitally interconnected ecosystem. Cloud-enabled distributed control will leverage these assets' network connectivity to enable sophisticated aggregation, coordination, and management at scale. Secure-by-design management software will enable greater operation and coordination of hundreds of thousands of distributed energy assets, virtual power plants, community microgrids, and other innovative energy systems, while integrating advanced cybersecurity control technologies.

**Building Energy Management Systems.** Software-defined resource management is transforming our energy ecosystem from the top-down, as well as the bottom up, with the Internet of Things and computer-based facility controls proliferating across our built environment. Advanced building energy management systems are improving comfort and well-being through the optimization of heating, ventilation, and cooling (HVAC) systems, as well as lighting systems, and the integration of "behind the meter" distributed energy resources, such as rooftop solar panels, on-site batteries, and generators.

**Electric Vehicles (EVs) & Electric Vehicle Supply Equipment (EVSE).** Electric vehicles and associated grid-integrated charging equipment (or EVSE) promise benefits beyond cheaper and more flexible forms of electrified transportation. Powered by secure and sophisticated distributed energy control systems, digitally-managed EVSE can enable smart charging, where utilities or consumers can manage the charging schedules of EVs to optimize grid load, reduce energy costs, or maximize alignment with modern energy sources. Similarly, EV batteries can be marshalled to be either local sources of backup electricity or citywide virtual power plants buttressing systemic resilience.



# Implementation Plan Reading Guide

This Implementation Plan is structured by key technology, with the first section comprising cross-technology initiatives. The fields presented for each initiative are:

**Goal** – The Goal associated with the initiative.

**Initiative Number** – A unique number associated with the specific initiative in the form of <Section>.<Initiative Number>.

**Initiative Title** – The title of an action that will support the overall Goal.

**Initiative Description** – An explanation of the activities associated with the action.

**Responsible Agency** – The Federal agency responsible for leading the initiative with other stakeholders. Responsible Agencies are responsible for coordinating with Contributing Entities under their initiative and working with ONCD to resolve any differences.

**Contributing Entities** – Where applicable, Federal departments or agencies that have a significant role in the development and execution of the initiative, including by contributing expertise or resources, engaging in complementary efforts, or coordinating on elements of a program. This is not intended to be a comprehensive list of all agencies with equities in an initiative.

**Completion Date** – Estimated completion date by quarter within the United States Government fiscal year.



## Section A: Cross-Cutting Issues

**Goal:** Enhance operational collaboration between government and energy sector partners

**Initiative Number:** A1

**Initiative Title:** Leverage and expand the scope of the Department of Energy's (DOE) Energy Threat Analysis Center (ETAC).

### Initiative Description

DOE will leverage and expand the scope of ETAC to the non-traditional energy space, ensuring ETAC fully integrates research and development (R&D), cyber operations, and threat intelligence across key stakeholders not incorporated into analogous existing or traditional institutions, such as the third-party owners and operators of the modern energy technologies outside of the utility ecosystem. This work will enable better coordination and response to emerging technology cyber threats in a way that preserves the appropriate separation, and does not jeopardize contractual relationships among the electricity subsector players. DOE will enable dissemination of threat and mitigation information along with vulnerability assessments with Sector Risk Management Agencies (SRMAs) and the National Coordinator for the Security and Resilience of Critical Infrastructure to key energy transition stakeholders.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER])

**Contributing Entities:** Office of the National Cyber Director (ONCD), Department of Commerce, Environmental Protection Agency (EPA), Cybersecurity and Infrastructure Security Agency (CISA)

**Overall Completion Date:** 4Q FY26

**Initiative Number:** A2

**Initiative Title:** Facilitate intelligence-informed briefings between the Intelligence Community (IC) and energy technologies industry groups.

### Initiative Description

Through the Sector Risk Management Agencies (SRMAs) and the National Coordinator for the Security and Resilience of Critical Infrastructure (in accordance with National Security Memorandum [NSM]-22), the Office of the Director of National Intelligence (ODNI) will regularly provide intelligence-informed briefings led by the IC to energy technologies industry groups. These groups should comprise infrastructure owners and operators, original equipment





manufacturers (OEMs), integrators, aggregators, and developers, through groups such as the Joint Office of Energy and Transportation’s Electric Vehicle Working Group (EVWG),<sup>2</sup> the Electric Vehicles and Charging Infrastructure Security Working Group (a cross-sector Critical Infrastructure Partnership Advisory Council [CIPAC] specifically focused on security and cyber security issues)<sup>3</sup>, and the National Charging Experience Consortium (ChargeX Consortium),<sup>4</sup> as well as Building Energy Management Systems (BEMS) industry groups. These discussions will enhance stakeholders’ understanding of relevant threats to and, as appropriate, vulnerabilities in or other areas of risk associated with, emerging energy technologies.<sup>5</sup>

**Responsible Agency:** ODNI

**Contributing Entities:** Department of Energy (DOE), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Joint Office of Energy and Transportation

**Overall Completion Date:** 4Q FY25

---

<sup>2</sup> “Electric Vehicle Working Group, Joint Office of Energy and Transportation,” Joint Office of Energy and Transportation, <https://driveelectric.gov/ev-working-group/>.

<sup>3</sup> “Critical Infrastructure Partnership Advisory Council (CIPAC),” Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac>.

<sup>4</sup> “ChargeX Consortium,” Idaho National Laboratory, <https://inl.gov/chargex/>.

<sup>5</sup> White House, “National Security Memorandum on Critical Infrastructure Security and Resilience,” <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>.



**Goal: Create communities of practice able to foster strategic unity, shared goals, and critical information flows**

**Initiative Number:** A3

**Initiative Title:** Develop and establish cyber and physical security common taxonomy and framework for linchpin technologies.

### **Initiative Description**

The Department of Energy (DOE) will establish a common taxonomy and consequence<sup>6</sup> modeling framework for current and emerging stakeholders (including distributed energy resources [DERs] owners, operators, original equipment manufacturers [OEMs], aggregators, and others) and describe their roles in supporting cyber and physical security. In partnership with industry, this will include defining roles and responsibilities for incident response and identifying opportunities to coordinate with the Electricity Subsector Coordinating Council (ESCC) on cyber mutual aid. Mutual Assistance or mutual aid is the sharing of resources (skilled personnel and/or equipment) from an unaffected entity or areas to those in need to expedite restoration. For emergency response during natural disasters, mutual assistance programs are frequently used by the electric industry, as well as states (via the Emergency Management Assistance Compact).<sup>7</sup> The electric sector is using this successful model for cyber defense, known as the ESCC Cyber Mutual Assistance (CMA) Program.<sup>8</sup> While this mutual aid program for cyber defense is a model led by the private sector, the Department of Energy will facilitate the conversation and set up the infrastructure for mutual aid models.

**Responsible Agency:** DOE (Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO] and Office of Cybersecurity, Energy Security, and Emergency Response [CESER])

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA)

**Overall Completion Date:** 4Q FY26

---

<sup>6</sup> The framework will leverage existing CCE work that can be found at “Consequence-Driven Cyber-Informed Engineering,” Idaho National Laboratory, <https://inl.gov/national-security/cce/>.

<sup>7</sup> Emergency Management Assistance Compact, <https://www.emacweb.org/>.

<sup>8</sup> “The ESCC’s Cyber Mutual Assistance Program,” Electricity Subsector Coordinating Council, <https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager.pdf?la=en&hash=827569B6061E85794AC581BF383C89E5D9DCD419>.



**Initiative Number:** A4

**Initiative Title:** Identify and map new energy stakeholders relevant to linchpin technologies' supply chains.

### **Initiative Description**

With a number of new entrants in the energy ecosystem, the expanding group of stakeholders in the community do not share clarity of purpose and risk calculus. Together with the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE) will identify and map stakeholders that can influence the development, deployment, and maintenance of new energy linchpin technologies and their supply chains, including integrators and manufacturers operating in the modern energy space, to ensure relevant cross-cutting activities and goals are appropriately understood and addressed.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO], EERE/Wind Energy Technologies Office [WETO], and Grid Deployment office [GDO])

**Contributing Entities:** CISA

**Overall Completion Date:** 4Q FY26



## Goal: Link digital energy infrastructure standards requirements to cross-cutting standards agenda

**Initiative Number:** A5

**Initiative Title:** Develop and publish implementation guidance for cybersecurity baselines for electric distribution systems and distributed energy resources (DERs).

### Initiative Description

The Department of Energy (DOE), in consultation with the National Labs, will develop a framework to unify existing disparate or absent cybersecurity standards and guidelines for digital energy infrastructure and their components into universally applicable guidance that can be implemented across all states. This framework will be developed in line with the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), leveraging DOE Cyber Baselines for Electric Distribution Systems and distributed energy resources (DERs), as well as the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)'s Cross-Sector Cybersecurity Performance Goals, where applicable.

The DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) partnered with the National Association of Regulatory Utility Commissioners (NARUC) to develop a set of cybersecurity baselines for electric distribution systems and DERs.<sup>9</sup> As states consider implementing new cybersecurity requirements, the potential of bespoke requirements grows, resulting in the potential for added complexity, confusion, and cost for entities that operate in multiple states.

A team of cyber, regulatory and industry stakeholders from across the energy sector were convened to develop baseline text and implementation guidance for using the baselines. This effort was broken into two phases. Phase 1 developed the baselines text which was published in early 2023 in collaboration with industry and state partners. Phase 2 is focused on developing the guidance that will be needed for states, utilities or DER entities to use or adopt the baselines.

**Responsible Agency:** DOE (CESER, Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO], EERE/Wind Energy Technologies Office [WETO], and Grid Deployment Office [GDO])

**Contributing Entities:** Office of the National Cyber Director (ONCD), CISA, Joint Office of Energy and Transportation, National Institute of Standards and Technology (NIST)

**Overall Completion Date:** 4Q FY26

---

<sup>9</sup> "Cybersecurity Baselines for Electric Distribution Systems and DER," National Association of Regulatory Utility Commissioners, <https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/#:~:text=The%20Cybersecurity%20Baselines%20are%20a%20vetted%20set%20of,distributed%20energy%20resources%20%28DER%29%20that%20connect%20to%20them.>



**Goal: Get “ahead of the curve” on cybersecurity practices for key currently- or soon-deploying technologies**

**Initiative Number:** A6

**Initiative Title:** Develop and drive the adoption of Secure-by Design and Default Principles.

### **Initiative Description**

The Cybersecurity and Infrastructure Security Agency (CISA), in consultation with the National Labs, will develop, test, and increase the adoption of CISA’s Secure-by Design and Default guidelines specific for digital energy infrastructure using the National Cyber-Informed Engineering (CIE) Strategy as reference. CISA will provide industry technical assistance on adoption and reporting, including the promotion of CISA’s Secure by Design pledge and the Department of Energy’s (DOE) Supply Chain Cybersecurity Principles.

**Responsible Agency:** CISA

**Contributing Entities:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER]), Joint Office of Energy and Transportation, National Institute of Standards and Technology (NIST)

**Overall Completion Date:** 4Q FY26



## **Goal: Develop a better understanding of potential cybersecurity risks with the next generation of energy technology**

**Initiative Number:** A7

**Initiative Title:** Develop a cybersecurity risk management framework for the integration of linchpin technologies.

### **Initiative Description**

The Department of Energy (DOE), in consultation with the National Labs, will develop a risk management framework that surveys and summarizes emerging cybersecurity risks for energy linchpin technologies, informed by existing gap analyses. This risk management framework will provide recommended actions for stakeholders to secure their systems.

Linchpin technologies, such as energy storage, inverter-based resources, and distributed control environments, all have interdependencies and system level coordination which impact their cybersecurity posture, such as cloud, mass orchestration, secure design standards, and artificial intelligence driven platforms. Securing those requires a consistent cross cutting digital transformation strategy for the national energy delivery system. Digital transformation represents a strategic response to these challenges by offering opportunities to enhance grid reliability, improve service delivery, and facilitate the transition to new energy technologies. This initiative will partner with industry stakeholders, to develop a national digital linchpin technology roadmap for deploying cybersecure and resilient integration technologies.

**Responsible Agency:** DOE (CESER, Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO], EERE/Wind Energy Technologies Office [WETO], and Grid Deployment office [GDO])

**Contributing Entities:** Office of the National Cyber Director (ONCD)

**Overall Completion Date:** 4Q FY26



## **Goal: Strengthen energy technology cybersecurity R&D community of practice capable of identifying priority R&D requirements**

**Initiative Number:** A8

**Initiative Title:** Baseline cybersecurity Research and Development (R&D) efforts related to new energy technologies.

### **Initiative Description**

A broad set of stakeholders is investing in cybersecurity R&D related to new energy technologies. To identify gaps and opportunities, a better awareness of the different projects is needed. Given the large number of projects and programs across new energy stakeholders – even within the Department of Energy (DOE) – this is a significant challenge. DOE, in consultation with the National Labs, will develop an initial view as a starting point for future refinements and expansion to additional stakeholders. Starting with the DOE National Laboratories, DOE will develop an initial baseline view of existing energy cyber R&D efforts across the DOE National Labs. This effort will include review and discussion by the DOE Cyber R&D community of practice and a determination of whether such information is actionable.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER] with the Office of Energy Efficiency and Renewable Energy [EERE])

**Overall Completion Date:** 4Q FY25



**Goal: Build cybersecurity considerations into the foundations of energy modernization, while ensuring it is flexible enough to accommodate not-yet-extant cybersecurity practices as they develop**

**Initiative Number:** A9

**Initiative Title:** Encourage and provide actionable guidance to sector stakeholders to procure digital energy systems that incorporate Secure by Design Principles.

### **Initiative Description**

The Cybersecurity and Infrastructure Security Agency (CISA) will encourage sector stakeholders to procure digital energy systems that incorporate Secure by Design Principles throughout product life cycles, minimize the operational costs for sustaining cybersecurity, and meet a baseline level of security through developing and issuing actionable guidance to integrators and end customers. In doing so, CISA will leverage secure supply chain principles such as those developed for the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Energy Cyber Sense.<sup>10</sup> If evident, CISA will identify opportunities for new incentive programs that may be helpful to drive adoption and equip stakeholders with guidance and questions to drive procurement decisions through Security by Demand, incorporating existing sector-specific procurement guidance.<sup>11</sup>

**Responsible Agency:** CISA

**Contributing Entities:** General Services Administration (GSA), DOE, Department of Transportation (DOT)

**Overall Completion Date:** 4Q FY26

---

<sup>10</sup> "Supply Chain Cybersecurity Principles," Office of Cybersecurity, Energy Security, and Emergency Response. <https://www.energy.gov/sites/default/files/2024-06/DOE%20Supply%20Chain%20Cyber%20Principles%20June%202024.pdf>

<sup>11</sup> "Securing Digital Energy Infrastructure," Idaho National Laboratory, <https://inl.gov/content/uploads/2023/11/FINAL-BESS-Supply-Chain-Security-Proc-Guidance-Sample-Contract-Terms-Compressed.pdf>.





## Goal: Develop a better understanding of potential cybersecurity risks with the next generation of energy technology

**Initiative Number:** A10

**Initiative Title:** Advance the Modern Energy Supply Chain

### Initiative Description

The Department of Energy (DOE) will establish a working group for Federal next generation energy technology integrators and importers of non-domestic digital energy infrastructure to evaluate the modification of equipment protection language in contracts for linchpin technologies, to include the integration of a right for the integrator or purchaser of the equipment to inspect internal (hardware and software) components provided. DOE and the Cybersecurity and Infrastructure Security Agency (CISA) will develop a software bill of materials (SBOM) and hardware bill of materials (HBOM) framework and prototype-acceptable contract terms and conditions. Language may include the use of recognized testing centers for equipment inspection and the removal of reverse engineering prevention clauses in imported equipment, as well as alignment with Secure by Design/Demand Principles.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Office of Energy Efficiency and Renewable Energy [EERE]/ Solar Energy Technologies Office [SETO] and the Grid Deployment Office [GDO])

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA), Office of the National Cyber Director (ONCD), Department of Commerce, General Services Administration (GSA)

**Overall Completion Date:** 4Q FY26

**Initiative Number:** A11

**Initiative Title:** Leverage Department of Energy (DOE) cybersecurity technical assistance capabilities to ensure federally funded modern energy projects take appropriate steps to plan for and mitigate the risk of cyber threats.

### Initiative Description

DOE will leverage existing cybersecurity plans in current and future infrastructure projects, and expand technical assistance, coordinating with existing efforts with Grid Deployment Office (GDO) and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) in Technical Assistance for Digital Assurance, and encouraging the application of demand for



secure design principles.<sup>12</sup> The technical assistance offered will be responsive to a rapidly changing regulatory landscape and cutting-edge equipment being tested for a feasible future allow list. Through the program, organizations will be matched with a national laboratory subject matter expert to focus on their key topical area, and a suite of tools which utilize Cyber-Informed Engineering and other operational tools to enhance the security of deployed modern energy projects.

**Responsible Agency:** DOE (GDO, CESER, Office of Energy Efficiency and Renewable Energy [EERE]/ Solar Energy Technologies Office [SETO])

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA), General Services Administration (GSA)

**Overall Completion Date:** 2Q FY26

---

<sup>12</sup> “Grid Resilience and Innovation Partnerships (GRIP) Program Technical Assistance Resource Center,” Department of Energy, <https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center>.

Technical Assistance and Training, Idaho National Laboratory, <https://inl.gov/csdet-technical-assistance-and-training/>.

“Energy Cyber Sense Program,” Department of Energy, <https://www.energy.gov/ceser/energy-cyber-sense-program> and <https://www.energy.gov/ceser/cybersecurity-testing-resilient-industrial-control-systems>.



## **Goal: Identify evolving landscape of energy system products bought and installed in the United States**

**Initiative Number:** A12

**Initiative Title:** Develop and implement an assessment of linchpin technologies supply chain-related cybersecurity risks.

### **Initiative Description**

Consistent with Supply Chain Cybersecurity Principles and Secure by Design Principles and in consultation with the National Labs, the Department of Energy (DOE) will conduct a holistic Digital Energy Infrastructure Supply Chain Assessment through a taskforce combining resources and processes across the Department of Commerce (Commerce), DOE, and the Cybersecurity and Infrastructure Security Agency (CISA). This assessment will include the identification and mapping of stakeholders that can influence the secure development, deployment and maintenance of energy linchpin technologies and their supply chains, including integrators and manufacturers operating in the modern energy space, to ensure relevant cross-cutting activities and goals are appropriately marketed and addressed.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Contributing Entities:** CISA, Office of the National Cyber Director (ONCD), Commerce

**Overall Completion Date:** 4Q FY25



## Goal: Develop a modern energy cybersecurity workforce

**Initiative Number:** A13

**Initiative Title:** Leverage the CyberCorps®: Scholarship for Service Program.

### Initiative Description

The National Science Foundation (NSF) will leverage the CyberCorps®: Scholarship for Service program and other cybersecurity workforce development infrastructure to investigate the potential for providing cybersecurity education scholarships with a service commitment to support cybersecurity in the federal government's electric sector, including electric distribution.

**Responsible Agency:** NSF

**Contributing Entities:** National Security Agency (NSA), Office of the National Cyber Director (ONCD)

**Overall Completion Date:** 2Q FY26

**Initiative Number:** A14

**Initiative Title:** Develop training and education modules for linchpin energy technologies.

### Initiative Description

The Department of Energy (DOE), in consultation with the National Labs, will develop curriculum and conduct training for linchpin technology security, configuration, and management. Through this training, owners and operators of linchpin technologies will be better prepared for cybersecurity incidents impacting operational technologies/industrial control systems with specific considerations of the architectures of digitally controlled modern energy technologies.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER] with Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Overall Completion Date:** 4Q FY26



## Section B: Batteries & Battery Management Systems

**Goal:** Create community of practice able to foster strategic unity, shared goals, and critical information flows

**Initiative Number:** B1

**Initiative Title:** Develop an interagency strategic plan for battery energy storage systems (BESS) and BESS controls through the creation of a joint working group.

### Initiative Description

The Department of Energy (DOE) will develop interagency strategic plan for battery energy storage systems (BESS) and BESS controls through the creation of an interagency working group across the Department of Homeland Security (DHS) and the Department of Energy (DOE) to develop cross-sector guidance for supply chain risk management and review, aligning that guidance with Secure by Design Principles and Cyber-Informed Engineering Design Principles; cybersecurity assessment and solution integration; interconnection; and safety management. This interagency working group will welcome new entrants to the battery ecosystem and foster clarity of purpose and shared risk calculus.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Grid Deployment Office [GDO], Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA), Office of the National Cyber Director (ONCD)

**Overall Completion Date:** 2Q FY26



## **Goal: Enhance operational collaboration between government and energy sector partners**

**Initiative Number:** B2

**Initiative Title:** Integrate Battery Energy Storage Systems (BESS) into cybersecurity exercise programs.

### **Initiative Description**

To address challenges with the battery ecosystem threat analysis picture not being consistently shared with stakeholders, the Department of Energy (DOE), in consultation with the National Labs, will integrate Battery Energy Storage Systems (BESS) into operational exercise programs for cybersecurity, such as GridEx and Liberty Eclipse. DOE will enable BESS operators to strategically participate in the program, such that cyber scenarios can be validated and remediated in future installations.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER])

**Contributing Entities:** Office of the National Cyber Director (ONCD), Department of Commerce, Department of Defense (DoD)

**Overall Completion Date:** 4Q FY26



## Section C: Inverters Controls & Power Conversion Equipment

**Goal:** Enhance operational collaboration between government and energy sector partners

**Initiative Number:** C1

**Initiative Title:** Develop guidance and best practices for the adoption and implementation of tools to increase cyber posture, detect, mitigate and remediate malicious anomalies in network connected inverters.

### Initiative Description

In partnership with industry and in consultation with the National Labs, the Department of Energy (DOE) will develop guidance and best practices for the adoption and implementation of assessment and monitoring tools or techniques to better detect, mitigate, remediate, and analyze anomalies found in network connected inverters for different installations including, but not limited to residential, plant, aggregated and utility scale. This guidance will include utility and non-utility owned assets. Prioritization can include inverters connected to the public internet and/or utilizing public infrastructure. Guidance will build off of existing guidelines and best practices, including National Institute of Standards and Technology Interagency or Internal Reports (NISTIR) 8498, *Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems*. Lessons learned from the guidance will then inform Cyber-Informed Engineering and Secure by Design efforts to eliminate common vulnerabilities and misconfigurations.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER] and Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Contributing Entities:** Office of the National Cyber Director (ONCD), Cybersecurity and Infrastructure Security Agency (CISA)

**Overall Completion Date:** 4Q FY26



## **Goal: Develop strategic cyber interconnection plan to enable guidelines to be pushed more regularly to the process of connection to the grid**

**Initiative Number:** C2

**Initiative Title:** Develop and implement a cybersecurity interconnection plan for inverter-based technologies.

### **Initiative Description**

Current processes for interconnecting inverter-based resources at the transmission level and the distribution level do not include sufficient cybersecurity reviews or study requirements. In addition, interconnection agreements do not adequately describe terms related to cybersecurity risk mitigation. Most existing practices depend on standards (e.g., Institute of Electrical and Electronics Engineers (IEEE) 1547-2018, IEEE 2800-2022) which do not include or adopt cyber as a core interconnection and operational issue.

To address these issues, the Department of Energy (DOE), in consultation with the National Labs, will develop cybersecurity-informed interconnection and design guidance for inverter-based resources and engage with stakeholder community for implementation. In doing so, DOE will leverage existing efforts to develop cybersecurity informed interconnection and design guidance for inverter-based resources and engage with the stakeholder community for implementation, using existing resources in FY25 and FY26 from DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and the Grid Deployment Office (GDO), such as Interconnection Innovation Exchange Program (i2X) and Cyber-Informed Engineering practices.

DOE will then implement the interconnection guidance to ensure regular enhancements to cybersecurity baselines above and beyond the pace of standards development, as well as regular coordination across state public utility commissions (PUCs), energy offices, and governors' offices to provide uniform, consistent, and deterministic implementation of cybersecurity requirements and best practices for modern energy technology.

**Responsible Agency:** DOE (CESER with Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO] & EERE/Wind Energy Technologies Office [WETO])

**Contributing Entities:** National Institute of Standards and Technology (NIST)

**Overall Completion Date:** 4Q FY26





## **Goal: Get “ahead of the curve” on cybersecurity practices for key currently- or soon-deploying technologies**

**Initiative Number:** C3

**Initiative Title:** Increase cybersecurity standards adoption among inverter-focused stakeholders.

### **Initiative Description**

Leveraging the Securing Solar for the Grid (S2G) program and the Grid Modernization Initiative’s (GMI) industry advisory board, the Department of Energy (DOE) will establish stakeholder groups focused on standards discussion. DOE will provide technical assistance to facilitate the adoption and implementation of standards related to inverter technologies (including manufacturing, installations, interconnection, and operations, among others), as well as Secure by Design Principles and the Cyber-Informed Engineering framework.

Through training, DOE will leverage current harmonization efforts for key inverter standards across entities to drive adoption of product security and safety guidelines, as well as operations standards aligned with consistent cyber-informed engineering design and operational cyber guidance and Secure by Design and Default Principles.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER] and Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), Office of the National Cyber Director (ONCD)

**Overall Completion Date:** 4Q FY26



## Section D: Distributed Control Systems

**Goal:** Harmonize integration and management of DERs through common data standards

**Initiative Number:** D1

**Initiative Title:** Review existing standards on data for advanced distribution management systems (ADMS), DER management systems (DERMS), microgrid controllers, and other DER integration software, and provide guidance for new standards as needed

### Initiative Description

DOE will review and update existing standards, or develop new standards, for the data requirement and data integration interfaces (i.e., application programming interfaces, or APIs) for advanced distribution management systems (ADMS), DER management systems (DERMS), microgrid controllers, and other distributed energy resources (DER) integration software in order to harmonize across DER and management systems and yield interoperability, efficiency, and reduction in cyber vulnerabilities for the grid.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Office of Electricity [OE], Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Contributing Entities:** Joint Office of Energy and Transportation

**Overall Completion Date:** 4Q FY26



**Goal: Build cybersecurity considerations into the foundations of distributed control systems rollout while ensuring they are flexible enough to accommodate not-yet-extant standards as they develop**

**Initiative Number:** D2

**Initiative Title:** Develop testing procedures and verification methodologies to ensure the standard data requirements are met in the integrated systems

### **Initiative Description**

The Department of Energy (DOE) will develop testing procedures and verification methodologies for the data requirement and data integration interfaces (i.e., application programming interfaces, or APIs) for advanced distribution management systems (ADMS), distributed energy resources management systems (DERMS), microgrid controllers, and other distributed energy resources (DER) integration software in order to provide industry with clear testing and verification methods for ensuring compliant vendor equipment.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Office of Electricity [OE], Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO])

**Contributing Entities:** Office of the National Cyber Director (ONCD), Joint Office of Energy and Transportation

**Overall Completion Date:** 3Q FY26



## Section E: Building Energy Management Systems

**Goal:** Get “ahead of the curve” on cybersecurity practices for key currently- or soon-deploying technologies

**Initiative Number:** E1

**Initiative Title:** Survey and harmonize cybersecurity standards across Building Energy Management Systems (BEMS).

### Initiative Description

Harmonization of cybersecurity standards for BEMS such as smart appliances and equipment; building telecommunications; security; and other sectors relevant to building energy control and security will ensure that cybersecurity approaches are right-sized to risk and consequence for the many relevant markets; establish and clarify cybersecurity standards that enable easy adoption by startups and innovators; and align with the Cybersecurity and Infrastructure Security Agency (CISA)’s Secure by Design and Default Principles and Cross-Sector Cybersecurity Performance Goals. In the BEMS domain, as is commonly the case, cybersecurity is primarily an IT/networking infrastructure issue and not an application issue. DOE Building Technologies Office’s (BTO) controls portfolio largely focuses on building-specific application-level standards and tools that sit one or more “layers above” IT/networking and are orthogonal to and agnostic of cybersecurity issues. Of course, real world BEMS installations comprise complete hardware/software stacks that include IT/networking.

Where BTO directly supports full-stack projects (e.g., Connected Communities) or promotes them (e.g., Small Building Controls Campaign), BTO, in consultation with the National Labs, will incorporate cybersecurity recommendations for hardware and software, network configuration, human factors, formal assessments, and general “hygiene” as developed by federal agencies such as the National Institute of Standards and Technology (NIST). BTO will also follow these recommendations in the innovative IT/networking work it undertakes as well as the latest guidance in secure application development in its application layer work, and will provide technical assistance on cybersecurity planning and implementation as needed.

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER] and Office of Energy Efficiency and Renewable Energy [EERE]/BTO)

**Contributing Entities:** CISA, NIST

**Overall Completion Date:** 4Q FY26



## **Goal: Diagnose building management system supply chain risk from a cybersecurity perspective and adopt appropriate mitigations**

**Initiative Number:** E2

**Initiative Title:** Identify most commonly-used components/platforms for Building Energy Management Systems (BEMS) today for conduct of vulnerability assessment.

### **Initiative Description**

The Department of Energy (DOE), in consultation with the National Labs, will leverage and expand the scope of its capabilities to de-risk building management system supply chains, which can be dependent on cyber-exposed subcomponents manufactured in countries of concern, contributing to uncertain amounts of risk. Much of this work will be conducted with partners, as the proprietary nature of supplier networks will be specific to technology developers and challenging to implement without their partnership. The work will build on a stakeholder map and tools developed by the cybersecurity team at Idaho National Laboratory (INL).

**Responsible Agency:** DOE (Office of Cybersecurity, Energy Security, and Emergency Response [CESER] and Office of Energy Efficiency and Renewable Energy [EERE]/ Building Technologies Office [BTO])

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA)

**Overall Completion Date:** 4Q FY26



## Section F: Electric Vehicles (EVs) & Electric Vehicle Supply Equipment (EVSE)

**Goal:** Create communities of practice able to foster strategic unity, shared goals, and critical information flows

**Initiative Number:** F1

**Initiative Title:** Support industry-led efforts to develop a public key infrastructure for plug-and-charge through the SAE Industry Technologies Consortia (SAE-ITC) Electric Vehicle Public Key Infrastructure Consortium (EVPKI Consortium) and other relevant activities.

### Initiative Description

*Plug and Charge* (PnC) is a method of initiating charging, whereby an Electric Vehicle (EV) charging customer plugs a connector into their vehicle and their identity is authenticated through digital certificates defined by ISO-15118, a charging session initiates, and a payment is transacted automatically, without any other customer actions required at the point of use. The *National Electric Vehicle Infrastructure Standards and Requirements* require the use of this protocol to enable interoperability of electric vehicle charging infrastructure.<sup>13</sup> In 2023, the SAE-Industry Technologies Consortia (SAE-ITC) launched the Electric Vehicle Public Key Infrastructure Consortium (EVPKI Consortium).

The Joint Office will provide cybersecurity expertise to the EVPKI Consortium from Federal research and development organizations to provide independent input and review of the proposed solutions. The Joint Office will deliver a Standards Cyber Assessment Report that details Public Key Infrastructure (PKI)-related technical and architectural cybersecurity risks which may exist in ISO 15118. This report will draw upon lessons learned from long-standing PKI implementations in finance and communications sectors. Additionally, the Joint Office will fund analyses of industry-preferred PKI implementations, and pre-competitive tools that close gaps in the existing plug-and-charge standards stack.

**Responsible Agency:** Joint Office of Energy and Transportation

**Contributing Entities:** Department of Transportation (DOT) (Volpe National Transportation Systems Center), Department of Energy (DOE)

**Overall Completion Date:** 1Q FY26

---

<sup>13</sup> See 23 CFR 680.108.



**Initiative Number:** F2

**Initiative Title:** Determine incident reporting responsibilities, harmonize those across existing reporting requirements, and develop tools to facilitate incident reporting between charging station operators, original equipment manufacturers (OEMs), state, local, Tribal and territorial (SLTT) transportation and energy officials, and Federal incident response agencies.

### **Initiative Description**

The Joint Office will identify relevant state, Federal, and private sector stakeholders involved with National Electric Vehicle Infrastructure (NEVI) cybersecurity event reporting. The Joint Office will analyze potential roles and responsibilities those stakeholders may have, and coordinate a common understanding for NEVI cybersecurity event reporting. The Joint Office will continue to engage stakeholders to deploy event reporting tools and templates to close any gaps in the NEVI cybersecurity event reporting ecosystem.

**Responsible Agency:** Joint Office of Energy and Transportation

**Contributing Entities:** Cybersecurity and Infrastructure Security Agency (CISA), Department of Transportation (DOT) (Volpe National Transportation Systems Center), Department of Energy (DOE)

**Overall Completion Date:** 1Q FY25



## **Goal: Accelerate the development of cybersecurity-focused technical standards and related guidance, including energy sector CPGs and NIST Privacy Framework profile for EV/EVSE**

**Initiative Number:** F3

**Initiative Title:** Develop industry guidance to meet 23 CFR 680.106(l) consumer data privacy requirement for electric vehicle supply equipment (EVSE).

### **Initiative Description**

Public electric vehicle charging infrastructure collects, processes, and retains potentially sensitive personal information, including but not limited to personal contact information, cardholder details, location data, energy consumption and transaction history. The sensitive nature of data handled by charging infrastructure has led to customer data privacy requirements within the NEVI Formula Program, which aim to safeguard consumer privacy by limiting the collection and use of personal information to what is essential for service provision.<sup>14</sup>

To address these requirements, the Joint Office will develop a National Institute of Standards and Technology (NIST) Privacy Framework profile for industry, leveraging the existing NIST Cybersecurity Framework Profile for Electric Vehicle/Extreme Fast Charging (XFC) Infrastructure as a model.<sup>15</sup> The framework will be a structured set of guidelines and best practices designed to help organizations manage and protect personal information effectively. It will encompass controls, guidelines, and practices aimed at ensuring that personal information is collected, stored, processed, shared, and disposed of in a manner that respects individual privacy.

**Responsible Agency:** Joint Office of Energy and Transportation

**Contributing Entities:** Office of the Director of National Intelligence (ODNI)/ National Counterintelligence and Security Center (NCSC), NIST, Department of Transportation (DOT) (Volpe National Transportation Systems Center)

**Overall Completion Date:** 4Q FY25

---

<sup>14</sup> See 23 CFR 680.106(l) (“**Customer data privacy.** Charging station operators must collect, process, and retain only that personal information strictly necessary to provide the charging service to a consumer, including information to complete the charging transaction and to provide the location of charging stations to the consumer. Chargers and charging networks should be compliant with appropriate Payment Card Industry Data Security Standards (PCI DSS) for the processing, transmission, and storage of cardholder data. Charging Station Operators must also take reasonable measures to safeguard consumer data.”).

<sup>15</sup> “NIST Interagency Report NIST IR 8473, Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure,” National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.pdf>.





## **Goal: Drive international adoption of secure modern energy technologies, including EV/EVSE**

**Initiative Number:** F4

**Initiative Title:** Promote the adoption of technical standards and guidance for electric vehicles (EVs) and electric vehicle supply equipment (EVSE) internationally.

### **Initiative Description**

In alignment with the National Standards Strategy for Critical and Emerging Technologies, the State Department will promote the adoption of technical standards and resilience worldwide through multi-lateral agreement to and engagement on EV/EVSE cyber security standards framework(s).

**Responsible Agency:** State

**Contributing Entities:** National Institute of Standards and Technology (NIST), Department of Energy (DOE) (Office of Cybersecurity, Energy Security, and Emergency Response [CESER], Office of Energy Efficiency and Renewable Energy [EERE]/Solar Energy Technologies Office [SETO]), Joint Office of Energy and Transportation, Cybersecurity and Infrastructure Security Agency (CISA)

**Overall Completion Date:** 1Q FY27



## **Goal: Ensure EVSE platforms are flexible enough to accommodate not-yet-existent standards as they develop**

**Initiative Number:** F5

**Initiative Title:** Develop an electric vehicle supply equipment (EVSE)-specific Cybersecurity Assessment Tool for EVSE original equipment manufacturers (OEMs) based on findings from EVSE Supply Chain Risk Evaluation, Analysis, and Mitigation study.

### **Initiative Description**

The Joint Office will transition findings from previously completed field testing into a portable test kit that EVSE stakeholders can use to rapidly evaluate EVSE and electric vehicle charging infrastructure (EVCI) security posture based on a cultivated hardware/software platform and provided testing methodology. The Electric Vehicle Charging Cybersecurity Analysis Tool will incorporate open-source security testing tools, such as those found in security-oriented Linux distributions, and combine them with customized toolsets and libraries to perform assessments on EVSE systems. Additionally, the initiative will integrate the software package with a low-powered, single-board computer for maximum portability. This tool will enable end users to evaluate multiple systems rapidly, and can be integrated with existing systems engineering processes to improve security testing as part of the systems development lifecycle. This initiative will result in a streamlined and extensible platform that can be used across the EVSE sector.

**Responsible Agency:** Joint Office of Energy and Transportation

**Contributing Entities:** Office of the Director of National Intelligence (ODNI)/ National Counterintelligence and Security Center (NCSC), Department of Transportation (DOT) (Volpe National Transportation Systems Center)

**Overall Completion Date:** 4Q FY25

**Initiative Number:** F6

**Initiative Title:** Mature industry-led cyber vulnerability discovery, coordination, and response in electric vehicle supply equipment (EVSE).

### **Initiative Description**

The Joint Office will mature EVSE industry-led cybersecurity vulnerability coordination and mitigation. Maturing this capability will enable EVSE stakeholders to receive, validate, fix, and disclose cybersecurity vulnerabilities in their products. The Joint Office is exploring the feasibility of creating financial incentives for electric vehicle charging infrastructure (EVCI) stakeholders to develop and document these capabilities, which are established cybersecurity best practices, through the use of their own bug bounty programs, which provide a method for



establishing ground rules and providing financial incentives for “white hat hackers” to submit vulnerabilities they find to the system owner, who then develop and deploy an appropriate mitigation. The Joint Office is also developing tailored guidance for the EVSE industry by adapting stakeholder specific vulnerability categorization (SSVC)<sup>16</sup>, and best practices for vulnerability management and coordinated vulnerability disclosure.<sup>17</sup>

**Responsible Agency:** Joint Office of Energy and Transportation

**Contributing Entities:** Department of Transportation (DOT) (Volpe National Transportation Systems Center)

**Overall Completion Date:** 1Q FY26

---

<sup>16</sup> “Stakeholder-Specific Vulnerability Categorization (SSVC),” Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc>.

<sup>17</sup> “The CERT Guide to Coordinated Vulnerability Disclosure,” [The CERT Guide to Coordinated Vulnerability Disclosure - CERT® Guide to Coordinated Vulnerability Disclosure](#).



## **Goal: Support agency procurement of secure electric vehicle-related infrastructure**

**Initiative Number:** F7

**Initiative Title:** Expand federal agencies' use of the General Services Administration's (GSA) electric vehicle supply equipment (EVSE) Blanket Purchase Agreements (BPAs) and/or indefinite delivery, indefinite quantity (IDIQ) contracts for the design, build, and installation of EVSE and their associated cybersecurity requirements.

### **Initiative Description**

GSA will expand federal agencies' use of its cost-effective EVSE acquisition solutions, such as BPAs and/or IDIQ contracts, and require all applicable, awarded platforms to meet security and privacy requirements as well as update a cyber supply chain risk management plan annually. Through agencies' use of these contracting vehicles, GSA ensures basic cybersecurity protections are in place for the EVSE installed at government buildings. As part of this work, GSA will also reduce the administrative burden on agencies and ensure agencies can more readily and efficiently adhere to the Federal Information Security Modernization Act.

**Responsible Agency:** GSA

**Overall Completion Date:** 4Q FY26



## Goal: Develop an EV charging cybersecurity workforce

**Initiative Number:** F8

**Initiative Title:** Identify cybersecurity workforce capability gaps in electric vehicle supply equipment (EVSE) stakeholder organizations and develop professional development tools to address those gaps

### Initiative Description

Cybersecurity workforce development among organizations within the Electric Vehicle (EV) charging sector is a barrier to cyber maturity. The Joint Office of Energy and Transportation seeks to close gaps in cross-domain expertise for both cybersecurity professionals (i.e., improve electric vehicle charging infrastructure [EVCI] protocol familiarity among cyber-SMEs) and EVCI professionals (i.e., improve familiarity with cyber security best practices among EVCI-SMEs). To accomplish this, the Joint Office will map EVCI job types to the National Institute of Standards and Technology (NIST) Workforce Framework for Cybersecurity (NICE Framework)<sup>18</sup> work roles. This mapping will inform training modules to bolster specific educational demands for staff positions at EVSE companies, and produce hands-on challenges within a virtual environment to test and hone cyber security skills for this segment of the EVCI workforce.

**Responsible Agency:** Joint Office of Energy and Transportation

**Contributing Entities:** Office of the National Cyber Director (ONCD), NIST, Department of Transportation (DOT) (Volpe National Transportation Systems Center)

**Overall Completion Date:** 1Q FY26

---

<sup>18</sup> “NIST Special Publication 800-181, Workforce Framework for Cybersecurity (NICE Framework),” National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>. NIST Special Publication 800-181, revision 1 provides a set of building blocks for describing the Tasks, Knowledge, and Skills (TKS) that are needed to perform cybersecurity work by individuals or teams. Through these building blocks, the NICE Framework enables organizations to develop their cybersecurity workforces and helps learners explore cybersecurity work and engage in learning activities to develop their capabilities



**Goal: Enable cyber defenders and managers to better understand systemic risks presented by EVSE integrations and identify opportunities for mitigation**

**Initiative Number:** F9

**Initiative Title:** Perform systems mapping and analysis of electric vehicle supply equipment (EVSE) integrations in complex environments to identify potential systemic risks.

### **Initiative Description**

The Department of Defense (DoD) will leverage the Office of the Under Secretary of Defense (OUSD) for Acquisition and Sustainment (A&S) Cyber Warfare's Cyber Risk to Mission Methodology to map and analyze electric vehicle (EV) and EVSE integration into a complex environment to identify risk to mission, assets, facilities, and infrastructure. DoD will identify and understand the mission dependencies and dataflows between the platform, EV, EVSE, installation/facility critical infrastructure, and commercial critical infrastructure. Analyzing the dependencies and dataflows, DoD will identify the vulnerabilities and risks imposed by these dependencies and interconnections of systems and their dataflow. DoD will integrate findings into a mapping of dependencies to vulnerabilities and risks to dataflows and potential attack surface/paths to enable an understanding of systemic risks of implementing EV/EVSE into our Nation's infrastructure and identify potential mitigations.

**Responsible Agency:** DoD (A&S)

**Contributing Entities:** Department of Energy (DOE), Department of Transportation (DOT) (Volpe National Transportation Systems Center), Environmental Protection Agency (EPA)

**Overall Completion Date:** 1Q FY27