

# State Energy Security Plan Optional Drop-In: IT/OT and Cyber Threat Overview

May 2022



This document was produced by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Argonne National Laboratory to aid states in the development of State Energy Security Plans (SESPs). States may choose to incorporate some or all of the provided material in their SESP (optional). States are encouraged to adapt or supplement the provided material as needed to better align with existing state roles, authorities, and plans; and to better address state-specific needs and situations. This document is not intended to be prescriptive or suggest non-statutory expansion of State Energy Office responsibilities.

## CYBER WITHIN ENERGY

Energy systems (electric, oil and natural gas) within {State}<sup>1</sup> use computing technologies to manage business systems and to control and monitor the processes and transportation of energy from production/generation to end use. The energy sector relies heavily on both information technology (IT) systems and operational technology (OT) systems.

OT systems include industrial control systems (ICS) that consist of purpose-built hardware, software, and data networks developed specifically for industrial customers. These systems were designed and built using tools and technology created before the Internet and technology boom of the late 90s. While these older systems are still in use, they have evolved and adopted newer technologies, including IT technologies built to allow internet connections.

Today the energy sector is technology driven, and these changes have resulted in many benefits including improvements to efficiency, resiliency, and flexibility. However, cybersecurity vulnerabilities and the capabilities of malicious actors have also changed over the past 20 years. Cyber threats are not limited to personally motivated individuals. Threats also come from well financed criminal and nation-state groups focused on profit, political gain, or power. The skill level and ability of these groups to compromise Internet-connected, Internet-adjacent, or even traditional ICS assets that were never designed to connect to the internet continues to grow.

## TECHNOLOGIES

OT systems interact with the physical environment or manage devices that interact with the physical environment. These systems monitor or control physical devices, processes, and events. Examples include:

- Energy Management Systems and Supervisory Control and Data Acquisition (SCADA)
- Oil refinery, gas processing and electricity generation distributed control systems (DCS)
- Pipeline pump/compressor stations and electrical substations
- General industrial control systems used in energy processes

A key area of distinction between IT and OT systems is that a cyber incident within energy OT systems can result in a physical consequence in addition to potential losses of data or damage to an organization's reputation. Some differences in the possible consequences/impact of an attack on an IT system compared with an OT system are described in Table 1.

---

<sup>1</sup> Text marked purple is intended for states to update/ tailor to their own unique needs.

**Table 1. Potential Impacts of a Cyber-attack on Energy Infrastructure**

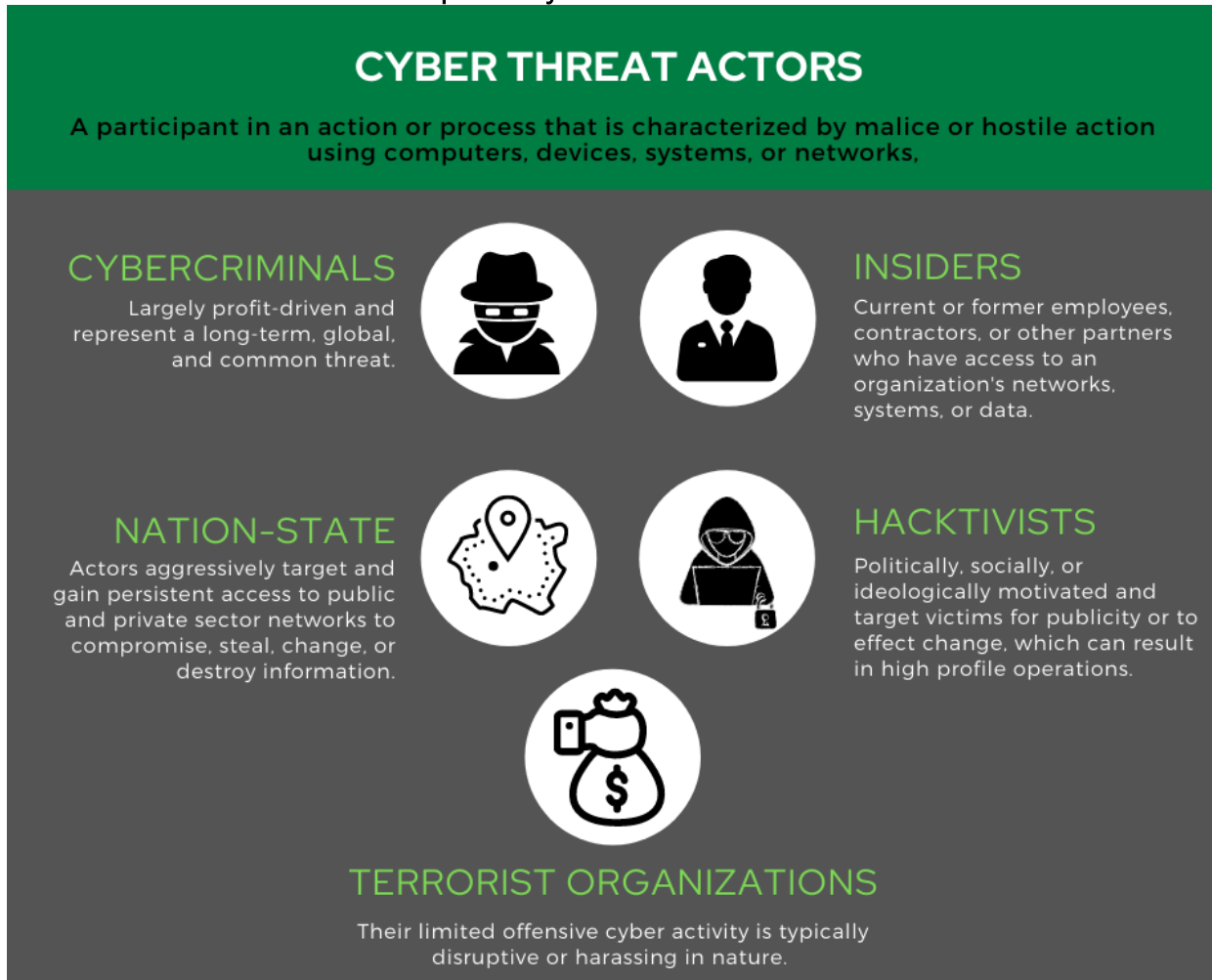
	Information Technology	Operational Technology
<b>Impacts</b>	<ul style="list-style-type: none"> <li>• Brand damage/ loss of confidence in company</li> <li>• Loss of personally identifiable information (PII)</li> <li>• Loss of business data</li> <li>• Customer/supplier payment issues</li> </ul>	<ul style="list-style-type: none"> <li>• Operator loses visibility into operations</li> <li>• Operator forced to switch to manual operations mode</li> <li>• Supply fails to meet demand</li> <li>• Disruption to basic daily activities – loss of power or access to fuel.</li> <li>• Health, safety, and economic impacts</li> <li>• Impacts from prolonged disruptions can cascade into larger consequences</li> </ul>

A cyber-physical event can cause loss of power or access to fuel, initiate prolonged cascading impacts, create potential risks to health and safety, and result in economic impacts to not just the company but to the people and businesses that rely on that energy. For cybersecurity best practices for industrial control systems, CISA and DOE created an [infographic](#) outlining key areas of consideration.

### **CYBERSECURITY THREATS**

The Annual Threat Assessment that the Office of the Director of National Intelligence (ODNI) released in 2022, emphasizes, as it has in the past, that cyber threats from nation states remain acute. ODNI’s concerns are focused on Russia, China, Iran, and North Korea, all of whom currently possess the ability to remotely damage infrastructure in the US or compromise supply chains. We know that adversaries – whether politically, socially, or financially motivated – are targeting our nation’s energy infrastructure and the digital supply chain. Graphic 1 shows categories of different kinds of threat actors and Graphic 2 shows different kinds of cyber attacks used by attackers.

Graphic 1. Cyber Threat Actors



The energy sector is uniquely critical because all of the other critical infrastructure sectors depend on power and fuel to operate. Unfortunately, this makes the Nation’s energy infrastructure an attractive target for cyber-attacks. Table 2 lists known cyber-attacks that have impacted energy systems. States are encouraged to add examples to this Table. All energy systems have vulnerabilities to cyber threats, 100% security is not possible. But many steps can be taken to harden OT systems to mitigate these threats.

Understanding the current and evolving threat landscape as well as possible consequences of a cyber-physical event can help state officials and energy owners and operators understand risks. Knowledge about risks can then be used to prioritize investments, such as purchases, staff resources, and training, based on the kinds of threats and vulnerabilities that pose the greatest risks to an organization. Investments can be focused on areas that can mitigate the highest risks. Because the majority of the nation’s critical infrastructure is owned and operated by private companies, both the government and private sector have a

common incentive to reduce the risks of disruptions to critical infrastructure. The [National Infrastructure Protection Plan](#) (NIPP) recognizes that public-private partnerships are vital to keeping critical infrastructure safe and secure, including from cyber attacks.




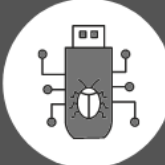



## CYBER ATTACK TYPES

In addition to understanding who cyber threat actors are, it is also important to understand the different methods those actors may use to compromise important systems, networks, and infrastructure. Common types of cyber-attacks are listed in Graphic 2.

Graphic 2. Cyber Attack Types

## CYBER ATTACK TYPES

An attack targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

<div style="margin-bottom: 20px;">  <p><b>SOCIAL ENGINEERING</b> The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.</p> </div> <div style="margin-bottom: 20px;">  <p><b>DENIAL OF SERVICE</b> Overloading a system through continual resource usage, that prevents legitimate use. Distributed Denial of Service attacks often use "botnets" or "Zombies" to scale an attack.</p> </div> <div>  <p><b>PENETRATION ATTACKS</b> The use of legitimate, publicly available resources on the Internet to check for servers, open ports, and other information that may allow unintended access into the system.</p> </div>	<div style="margin-bottom: 20px;">  <p><b>MALWARE</b> A computer program that is covertly placed onto a computer or electronic device with the intent to compromise the confidentiality, integrity, or availability of data, applications, or operating systems.</p> </div> <div style="margin-bottom: 20px;">  <p><b>VIRUSES AND WORMS</b> Introduction of self-propagating or initiated malware into a system through methods such as malicious email attachments, USBs, etc. that seeks to monitor, access, delete, or alter data for nefarious use.</p> </div> <div style="margin-bottom: 20px;">  <p><b>TROJANS</b> Malware which allows "back door" access into a system. This allows an attacker to have a longer reconnaissance through continual check-ins.</p> </div> <div>  <p><b>RANSOMWARE</b> Maliciously locking up data or systems and demanding payment of a fee (ransom) or other concessions to unlock the data or systems.</p> </div>
---	---

## ICS CYBER ATTACK HISTORY / EXAMPLES

Table 2 includes several notable examples of cyber attacks perpetrated by various threat actors. States can add additional examples as appropriate.

**Table 2. Industrial Control System Cyber Attack Examples**

Attack Name	Physical Target	Method	Impact / Implication
<b><u>Stuxnet (2010)</u></b>	Nuclear Facilities (Iran)	Stuxnet was the first publicly known malware to specifically target control systems with the intent to damage physical infrastructure. The malware was especially notable due to its covert nature - presenting fake data to operators while hiding operations underway.	Proof that hardware is an equal threat vector and that ICS systems are targets.
<b>BLACKENERGY 3 (2015)</b>	Regional electricity distribution company (Ukraine)	The attackers likely spent an extended period of time doing reconnaissance before executing their final attack. Attackers used spear phishing emails, multiple variants of malware, and manipulation of documents as part of a broad campaign. After gaining initial access, they captured valid credentials and leveraged those credentials to access electric power SCADA systems. Successful penetration of the OT systems enabled them to shut down and disable portions of the distribution power grid.	Approximately 225,000 Ukrainian power customers lost power. Manual black start <a href="#">required</a> .
<b>CRASHOVERRIDE (2016)</b>	Electrical substation (Ukraine)	Leveraged previous successful ICS attacks such as Stuxnet, Havex, and BLACKENERGY 3, as learning mechanisms to develop industrial system malware that could work on multiple infrastructures without a human operator (unlike BLACKENERGY 3).	Kiev, Ukraine experienced a one-hour power disruption. The attack failed to accomplish apparent goals, but it was a demonstration of the attacker's ability to accomplish automated cyber attacks on critical infrastructure.
<b>Triton / Trisis (2017)</b>	Petrochemical Facility (Saudi Arabia)	The first publicly known attack on a Safety Instrumented System (SIS), a system of last resort intended to protect lives by triggering emergency shutdowns of industrial processes if unsafe conditions are reached. Attacker gained access and deployed malware directly onto the SIS to gain <i>full access to the SIS without plant operator knowledge</i> . The malware installation triggered a failsafe that activated the SIS.	Shut down plant operations at a petrochemical facility, triggering a full investigation.  Preventing safety mechanisms from performing their intended function can result in physical consequences.

<u><b>Unnamed Attack (2019)</b></u>	U.S. electric grid	A cyber-attack temporarily created blind spots between a control center and a number of remote generation sites in the western U.S. by exploiting a vulnerability in a technology vendor's firewall.	Denied reliable communications between a control center and the power generation controlled
<u><b>EKANS / Snake (2020)</b></u>	ICS operations (Enel and Honda)	<a href="#">Ekans/Snake</a> utilized popular ransomware attack methodology, but targeted control system processes instead of more common targets. This malware contains static lists to automatically kill known processes run by ICS.	First known ransomware that targeted ICS/OT. Manufacturing operations disrupted on 3 continents after victims decided to suspend ICS/OT operations.
<u><b>Colonial Pipeline Ransomware Attack</b></u>	U.S. petroleum pipeline	<ul style="list-style-type: none"> <li>▪ Darkside Ransomware</li> </ul> <p>The cyberattack targeted Colonial Pipeline's IT network, prompting the company to proactively shut down pipeline operations as a precaution.</p>	<p>Fuel stopped flowing, affecting Southeast and MidAtlantic states who are heavily dependent on the Colonial Pipeline for their fuel. Limited alternatives to the pipeline.</p> <p>Consumer panic buying, further limited supply which was also exacerbated by tanker truck driver shortage</p>
<i>[Additional attacks]</i>	...	<ul style="list-style-type: none"> <li>▪ <i>[Method]</i></li> </ul>	<ul style="list-style-type: none"> <li>▪ ...</li> </ul>

## FEDERAL AND STATE CYBER INFORMATION SHARING

Cybersecurity information sharing is vital and ideally is bi-directional. This includes sharing cybersecurity best practices, guidance, and trends; information on emerging cyber threats and vulnerabilities affecting energy sector stakeholders; and real-time information sharing during the response and recovery stages following a cyber event.

Robust, timely, actionable information is crucial to all partners because each has a unique role to play in protecting critical infrastructure against cybersecurity threats as well as participating in a coordinated response should a cyber incident occur.

{State} engages in information sharing by {...describe the mechanisms by which the state receives, analyzes and/or shares information with energy and emergency officials and energy industry partners. This may include various state entities performing a wide range of activities.}

Below are a few examples, but by no means an exhaustive list.

- Actively monitoring announcements and alerts from Information Sharing and Analysis Centers, or “ISACs”
- State information-sharing processes are well-defined and documented {location}
- Cyber information sharing mechanisms are tested through exercises
- Facilitate or attend threat briefings (unclassified or classified)
- Designation of {Employee} as “cyber lead” to keep current on cybersecurity news as it pertains to the energy sector and to relay high priority items or alerts to leadership
- Fusion center practices may include bi-directional information sharing with the sector, briefings, or other outreach
- Public utility commission holds formal or informal discussion with utilities about cybersecurity strategies, plans and challenges
- State facilitates informal energy CISO or industry group calls to share cybersecurity updates, trends, and questions
- Distribution of actionable indicators or detection signatures of malicious activity, vulnerability information, courses of action (to proactively defend or to stop and remediate an attack), and cyber threat intelligence.
- Incentivizes industry participation in federal cyber information sharing programs



## CESER-SUPPORTED RESOURCES FOR ASSESSING CYBER MATURITY

SEOs should be aware of available tools to assess and enhance cyber maturity.

The Department of Energy’s [Cybersecurity Capability Maturity Model \(C2M2\)](#) enables organizations to voluntarily measure the maturity of their cybersecurity capabilities in a consistent manner through a publicly available tool.

The American Public Power Association (APPA) developed the [Public Power Cybersecurity Scorecard](#), an online self-assessment tool for municipal utilities to evaluate their cybersecurity programs and overall posture. This tool is based on C2M2 and builds upon the assessment with additional resources.

The National Rural Electric Cooperative Association (NRECA) developed the [RC3 Cybersecurity Self-Assessment](#). The assessment, available either hardcopy or online, is designed to help cooperatives understand their cybersecurity posture and is part of the larger [Rural Cooperative Cybersecurity Capabilities \(RC3\) Program](#). The RC3 program develops and provides tools and resources focused on improving the cybersecurity capabilities of cooperatives. The program also provides opportunities for collaboration, education, and training.

The National Association of Regulatory Utility Commissioners (NARUC) has developed a suite of cybersecurity resources for public utility commissions (PUCs), including [Understanding Cybersecurity Preparedness: Questions for Utilities](#). SEOs should be aware of NARUC’s cybersecurity resources by virtue of their energy sector relevance. These resources may be useful in preparing an SEO for a conversation with their state’s PUC about cybersecurity, the overall maturity levels of the state’s regulated utilities, and where gaps need to be addressed.

Resource	Members	Description
<a href="#">Multi-State Information Sharing and Analysis Center (MS-ISAC)</a>	List state members (who may convey information relevant to energy)	The MS-ISAC is dedicated to improving the overall cybersecurity posture of state, local, territory and tribal (SLTT) governments, and is a resource for information on cyber threats to critical infrastructure. {State} members of the MS-ISAC can share threat information to the energy sector when appropriate.
<a href="#">Electricity Information Sharing and Analysis Center (E-ISAC)</a>	Electricity owners and operators in North America  Approved individuals at states with energy emergency response roles	The E-ISAC provides information and resources to help the North American electricity industry prepare for and defend against both cyber and physical security threats.

<a href="#">Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC)</a>	Public and private ONG companies, select collaborators and partners, subject to membership requirements.	The ONG-ISAC serves as a central point of coordination and communication to aid in the protection of exploration and production, transportation, refining, and delivery systems of the oil and natural gas (ONG) industry, through the analysis and sharing of trusted and timely cyber threat information, including vulnerability and threat activity specific to ICS and SCADA systems.
<a href="#">Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC)</a>	Natural gas utility companies.	The DNG ISAC serves natural gas utility (distribution) companies by facilitating communications between participants, the federal government and other critical infrastructures.
<i>[State Fusion Centers]</i>		List and describe all applicable state fusion centers
<i>[Additional State-identified information sharing]</i>		List additional information sharing resources, as identified by the state

Note: The U.S. Department of Energy’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER) intends to expand this cyber-specific state resource based on state feedback and needs in late 2022.