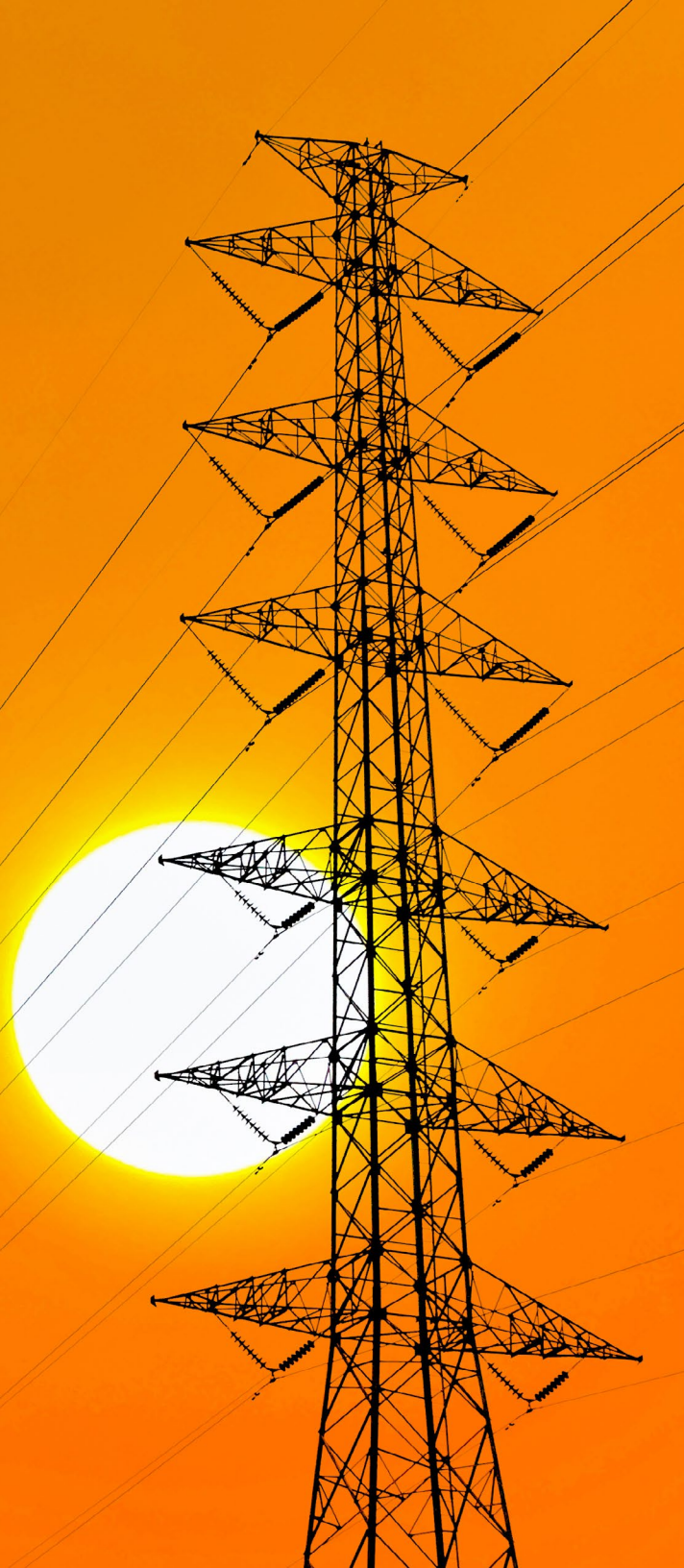
SIEMENS

HOW TO PREPARE FOR AN UNPRECEDENTED OPPORTUNITY TO RECEIVE GOVERNMENT FUNDING

Upgrading your **cybersecurity infrastructure**



usa.siemens.com/electric-power-networks
siemensci.us@siemens.com

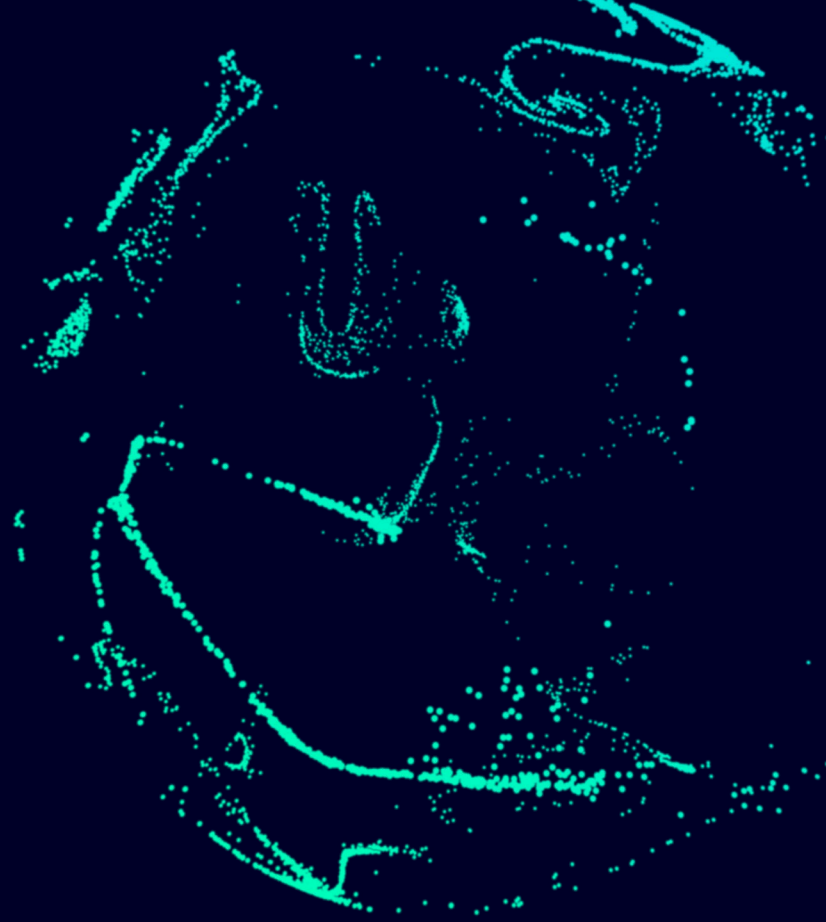


Table of contents

Cybersecurity threats **and opportunities**

Fortifying cybersecurity in publicly owned utilities has never been more urgent. As the incidence of cyberattacks **has swelled to historic levels**, so has the prevalence of **hacks on public utilities**. Now is the time to invest in modernizing and protecting your networks. Thankfully, the new critical infrastructure bill provides funding for exactly that, with financial incentives available immediately.

Included in the **$1.75 trillion bill is $10 billion for grid infrastructure, resiliency and reliability**. Additionally, there is **$1 billion** to help local governments protect sensitive systems from cybercriminals, along with another $100 million for cyber response and recovery. That money will flow largely through state funding.

The legislation also earmarks **$65 billion for rural broadband access**, with $14 billion of that aimed at reducing internet costs in underserved rural communities.

It further **directs the Federal Energy Regulatory Commission (FERC) to establish incentives** for utilities to invest in advanced cybersecurity technology.

> "(The infrastructure bill provides) a huge amount of funding to allow us to build the kinds of grids, the resilient grids, the cybersecure grids, that we need in our country."
>
> – U.S. Department of Energy Deputy Secretary David Turk

What this means for **utilities**

Passage of the infrastructure bill means money and funding is immediately available for utilities. **This includes grants**, which will be managed by the Department of Energy or the Department of Agriculture, separate from the accelerated depreciation incentives proposed by FERC.

In April 2021, the Department of Energy launched a **100-day action plan** designed to strengthen cybersecurity for critical infrastructure across the country. At least 150 electric utilities have already adopted or committed to adopting Operational Technology and Industrial Control Systems technology improvements during that window. The ICS initiative's strongest focal points are on operator detection, mitigation and forensic capabilities.

The initiative includes a **host of suggested evaluation considerations**, including:

- **Continuous network cybersecurity monitoring, detection and response capability**
- **A collective defense framework able to share data with the federal government**

- **Systems that do not store sensitive data, or that otherwise protect/anonymize sensitive data**
- **Dynamically updatable technology capable of detecting a wide range of threats and unauthorized activity**

States like California and Texas are already mandating improvements to the grid, threatening utilities with potential damages if outdated infrastructure leaves customers without power during an emergency. Between the benefits of being proactive and the increasing risks of failing to do so, there's no reason to wait to implement your cybersecurity action plan.

How to **take advantage**

To take advantage of the financial incentives on the table, you must meet certain guidelines. You'll also need to document the steps you take, so be sure your cybersecurity action plan meets the standards.

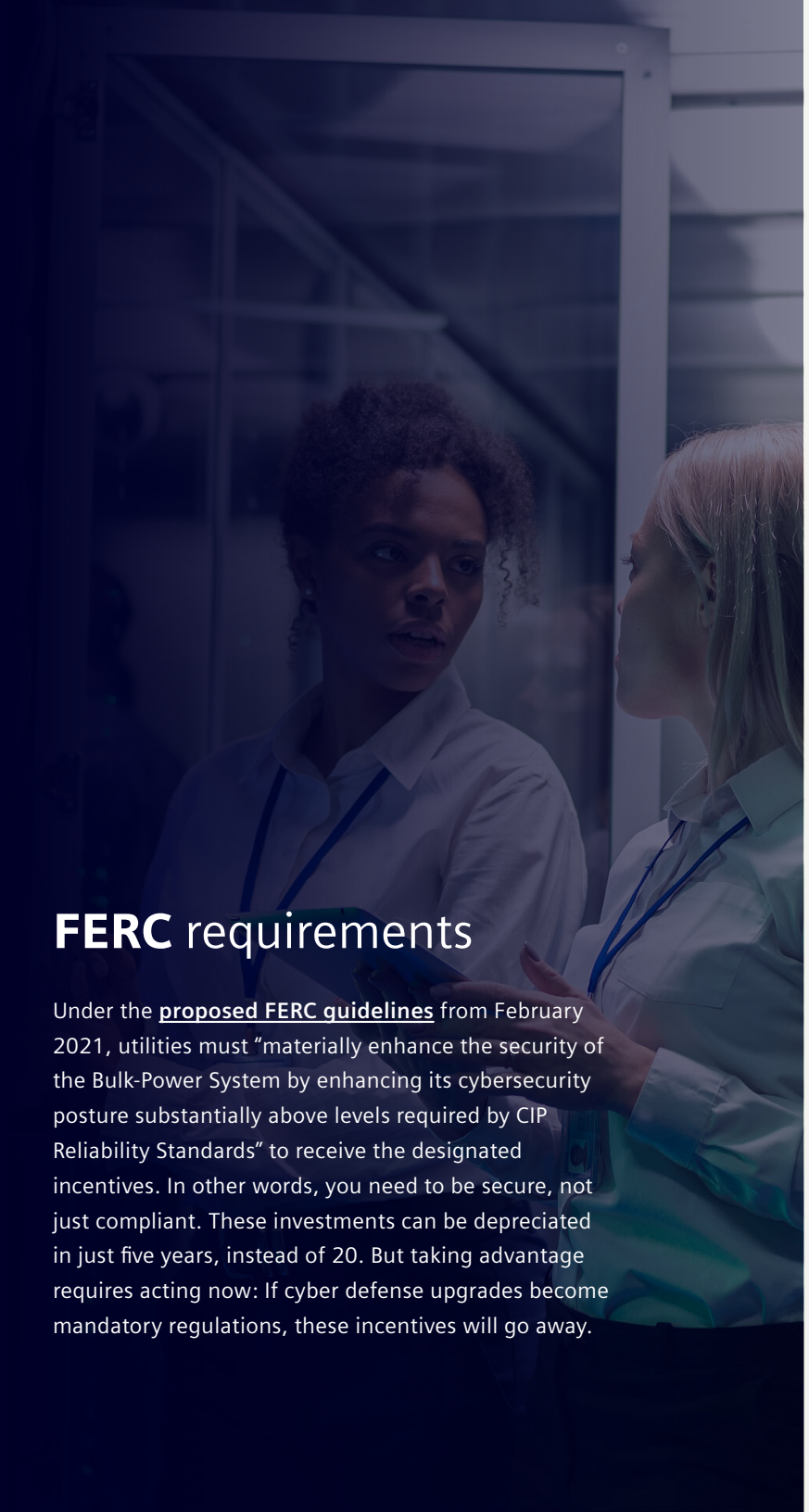
Cybersecurity **readiness plan**

1. **Obtain buy-in from key stakeholders within the organization.**
2. **Choose a standard or requirement to adhere to.**
3. **Devise a plan.**
    a. If any Cybersecurity Capability Maturity Model (C2M2) guidelines from DOE will apply, conform to that plan.
4. **Conduct a cyber asset audit based upon standard.**
5. **Perform cyber vulnerability based upon standard and organization's cyberplan.**
6. **As a result of audit/scan, devise a plan to mitigate any discovered/known issues:**
    a. Network design (i.e., close unused ports, network segmentation, implement encryption where possible).
    b. Establish password management policy for assets/users.
    c. Do firmware updates/upgrades on network assets for each segment of the network.
    d. Perform software updates on network assets for each segment of the network.
    e. Align groups for deployment of upgrades and institute advanced training to minimize field time.
    f. Develop a "Defense in Depth" plan (Decide on Intrusion Detection, Intrusion Prevention, and NGFW platforms and have management approval for said approach).
    g. Create a patch management program.
    h. Move any issues to a GAP policy and establish timeline for resolution.
    i. Identify remote access needs for employees and contractors.
    j. Develop an incident recovery plan.

Cybersecurity **enablement plan**

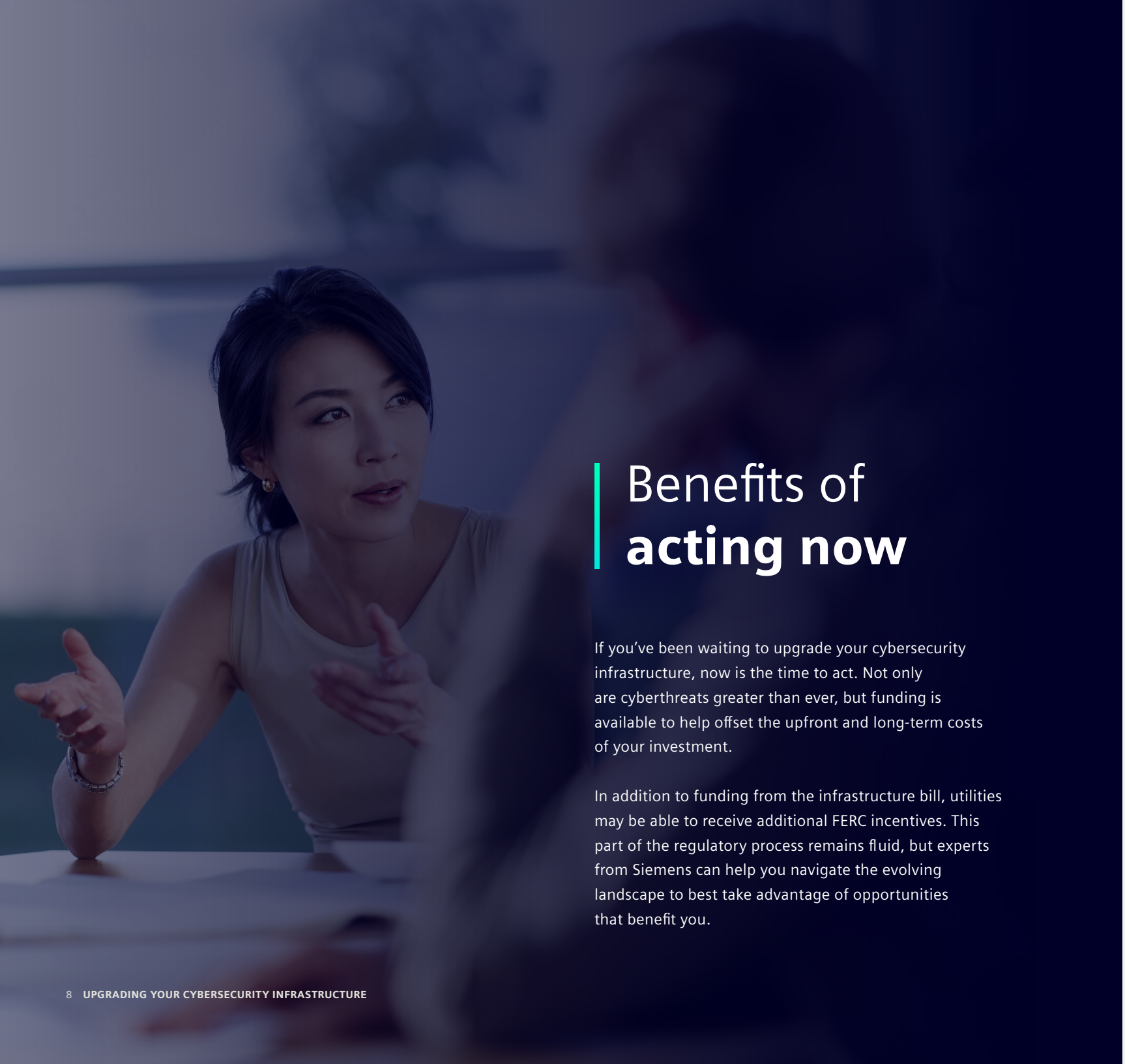
Integrating into your operations

1. **Have test lab to run preferred cybersecurity application(s) and run test plan. Eliminate any variables and implement final test plan.**
2. **Train responsible field technicians on implementation procedures.**
3. **Establish an implementation timeline on High Risk Assets, then Medium Risk Assets, followed by Low Risk Assets (if applicable).**
4. **Begin a monthly audit to ensure application is deployed and running as planned. Record network functionality. If any alarms are raised, investigate and isolate the issue(s) from the network.**
5. **Create an annual process for cybersecurity audits and vulnerability scans from an independent entity.**



FERC requirements

Under the **proposed FERC guidelines** from February 2021, utilities must "materially enhance the security of the Bulk-Power System by enhancing its cybersecurity posture substantially above levels required by CIP Reliability Standards" to receive the designated incentives. In other words, you need to be secure, not just compliant. These investments can be depreciated in just five years, instead of 20. But taking advantage requires acting now: If cyber defense upgrades become mandatory regulations, these incentives will go away.



Benefits of **acting now**

If you've been waiting to upgrade your cybersecurity infrastructure, now is the time to act. Not only are cyberthreats greater than ever, but funding is available to help offset the upfront and long-term costs of your investment.

In addition to funding from the infrastructure bill, utilities may be able to receive additional FERC incentives. This part of the regulatory process remains fluid, but experts from Siemens can help you navigate the evolving landscape to best take advantage of opportunities that benefit you.

Potential **FERC incentives**

These incentives are available for facilities making voluntary upgrades to CIP standards or meeting the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. These additional opportunities are likely to disappear when the security benchmarks being promoted become mandatory. Upgrading to a higher level of security today will not only get you ahead of impending regulations — it will benefit you financially.

Return On Equity for applicable investments

- **200-basis point increase in ROE**
- **Need to submit plan for investments, allocations**
- **Capped at zone of reasonableness**
- **Eligible for one, not both incentives**

Deferred cost of recovery

- **Three categories of expenses:**
  - **Third-party provision of software**
  - **Software/computer networking services**
  - **Risk assessment, system review and implementation**
- **Amortized over five-year period**
- **Not applicable to prior or continuing costs**

Increased risk in the energy sector

The **Colonial Pipeline ransomware attack** in May 2021, showed how vulnerable major players in the energy industry can be to cyberattacks and how widely the consequences can ripple. Utilities provide vital daily services to millions of people. A diverse and dispersed energy infrastructure that is increasingly digitally interconnected offers more entry points to hackers, with the potential to cause exponentially more damage.

> As the sector evolves … we know that it's become an increasingly attractive target to our cyber adversaries."
>
> – Kate Marks, Acting Deputy Assistant Secretary of Infrastructure, DOE Office of Cybersecurity

It's apparent the energy sector is an attractive target. And even if an attack is managed relatively quickly, the reputational damage from a public incident can stick to your name for much longer. The best cybersecurity strategy is one that helps you avoid ever being in the news in the first place.

That strategy requires protecting yourself on several fronts. Utilities need rugged, durable equipment with maximum flexibility and easy maintenance. They also require upgrades that can fit seamlessly into the existing system architecture. A **Cybersecurity by Design** approach is comprehensive and works to prevent breaches, eliminating the need to repair and restore damaged systems.

Coupled with **Operationalizing Cybersecurity** — a proven approach to establishing and maintaining a comprehensive cybersecurity program — ensures that utilities can protect their operational and business continuity. This proven approach puts ideas into action through implementation of cybersecurity frameworks, policies, processes, and technologies to secure Operational Technology networks and the Industrial Control Systems that run them.

RUGGEDCOM: A complete, proven solution for today and tomorrow

The cybersecurity landscape is always shifting, but between the escalating threats and the investment funding now available through the infrastructure bill, the situation is developing quickly. With so many moving parts, tackling each aspect of modernizing your systems takes a lot of time and effort.

Siemens is an established leader in industrial communication and cybersecurity, initiating the Charter of Trust in 2018 to help combat cyberattacks. In 2020 alone, we introduced two new evolutions of products with faster chip sets, increased cybersecurity capabilities, and improved network visibility for the end user. Siemens not only uses open system architecture to incorporate best-in-class third-party apps, we also integrate forward-looking apps into our newest products. By complying with both U.S. and international standards for open-facing platforms, Siemens helps you keep options open and costs down.

Whether you're looking to upgrade your existing infrastructure or are starting from a blank slate, intelligent cybersecurity demands an end-to-end solution. From system assessment to design consultation, RUGGEDCOM provides on-site training and support, and our professionals are uniquely qualified to help utilities draw their own road map to secure their grid.

Regardless of your existing infrastructure, RUGGEDCOM's open system architecture provides proven, seamless integration in substation and control room networks. Its modular design makes the technology easy to upgrade as your needs change and quick to deploy as real-world conditions demand.

With hardware refreshed in 2021, RUGGEDCOM delivers affordability, universality and a future-proof cybersecurity solution for utilities. Be sure to ask us about our Trade-in/Trade-Up program and our new **10-year warranty option**.

Securing your networks with RUGGEDCOM is a down payment on your cybersecurity future. With the financial incentives currently available, there has never been a better time to invest in protecting yourself. Contact us today to see what RUGGEDCOM can do for your networks.

Contact us