BLACK & VEATCH

Pathway to Federal Cybersecurity Compliance

Cybersecurity Compliance for Reliable, Resilient and Sustainable
Federal Critical Mission Facilities and Infrastructure

Contents

Introduction

The current landscape in the cybersecurity environment is one where adversarial ingenuity, technology and fiscal motivations are both increasingly dynamic and dangerous to our Nation's defense and commercial infrastructure. Today's demand dramatically outweighs the supply of cleared, certified and experienced cybersecurity professional and services. Currently, it is estimated that there are only 65% of the required professionals to meet the cybersecurity crisis.

As the connected world grows exponentially, there are around 200 billion devices connected to cyber space. This means that cybersecurity is of the utmost importance. A majority of the world now accesses the Internet via mobile devices. Meanwhile, mobile apps request a plethora of personal data. It has been said that data is now more valuable than oil because of the insight and knowledge that can be extracted from it. It is scary how easy it is for cybercriminals to hack your accounts and breach your business once they collect this information. So, cybersecurity for all connected devices is very important, as it protects all categories of data from theft and damage. The annual loss of intellectual property in the US is estimated at $600B.

The Black & Veatch team is ready to offer these services now. We have a robust pipeline of trained and certified personnel made up of cleared and uncleared professionals, tailored to meet the mission requirements of clients, and statutory requirements of the federal government.

What is Cybersecurity?

Cybersecurity is the protection of critical information at rest, in transit, and during duplication:

- At rest on media and in hard drive — it is important that is not copied or changed without proper authorization
- In transit — ensure availability of data systems and confidentiality that only approved recipients can receive the information
- During duplications — protecting the integrity and security of the data

U.S. Federal Government Priorities

- Protecting against breaches and downtime
- Keep our Nation safe from Nation-state adversaries, transnational terrorist groups and criminal activity
- Protect the Cyber warfighter mission through detection and deterrence of cyber threats
- Migrate to a Zero Trust Architecture (ZTA)

As reported by the U.S. Government Accountability Office in March 2023, the White House issued the National Cybersecurity Strategy, describing five pillars supporting the Nation's cybersecurity:

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience
- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals

Critical mission infrastructure is more than facilities and programs you can see, it is the strategic detection and deterrence of any threat. At Black & Veatch, our mission is to provide mission assurance for clients seeking to protect our nation, eliminate threats, and strengthen its systems so they work no matter what.

Critical facilities, programs and infrastructure must be designed and built to fulfill its purpose on day one. It must remain fully operational for years and decades to come through the full range of today and tomorrow's threats. Regardless of whether these threats consist of attempted breaches of secure areas, assaults using long-ranged weapons, cyber-based intrusions, or chemical, biological, radiological and nuclear (CBRN) attacks originating from Nation-state adversaries, transnational terrorist groups, or criminal activity, Federal contractors must have the knowledge and experience to provide our clients solutions for a secure and reliable mission.

Cybersecurity Threats

The current Administration has made cybersecurity a top priority at all levels of government. To advance its commitment, enhancing the Nation's cybersecurity resilience is a top priority for the Department of Homeland Security (DHS). The **President's Budget** includes approximately $12.7 billion of budget authority for civilian cybersecurity-related activities, an increase of 13 percent over the prior year. DHS' agency, Cybersecurity and Infrastructure Security Agency (CISA) is the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience. Defending our Nation against ever-evolving cyber threats and attacks is at the core of CISA's mission.

In addition to national priority increasing investment in cybersecurity, they have also increased enforcement. The current administration has signaled that it views national cybersecurity as an important enforcement priority. In May 2021, the President signed an Executive Order on Improving the Nation's Cybersecurity, stating that "the Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems." That same month, the U.S. Deputy Attorney General ordered a comprehensive cyber review "aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats." The Civil Cyber-Fraud Initiative arose from that review.

On October 6, 2021, the U.S. Deputy Attorney General announced a new Civil Cyber-Fraud Initiative through which the Department of Justice (DOJ) will utilize the False Claims Act (FCA) as a tool to enforce cybersecurity standards required of federal contractors and grant recipients. Specifically, the DOJ will target companies and individuals that allegedly misrepresent their cybersecurity practices or protocols to win a federal contract or grant or that knowingly submit claims to the government for payment while in violation of regulatory or contractual cybersecurity requirements.

Market Drivers

- **Societal:** Cyber threats are causing interruptions to personal information and safety
- **Economic:** Cyber threats are causing interruptions to our Nation's economy
- **Political:** Prevention of warfare, detention and detection of potential threats
- **Technological:** Cyber threats to technology infrastructure for citizens and organizations
- **Financial:** Intellectual property losses and increased costs due to security breaches

As a trusted advisor for DoD and Federal civilian agencies, Black & Veatch supports its clients through this change. We know and understand firsthand how to apply world-class capabilities to ensure the highest level of cybersecurity on facilities, programs, and infrastructure with critical national interest.

Types of Cyber Threats and Advisories

- **Malware, Phishing, and Ransomware -** Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals and large organizations. Malware is any software used to gain unauthorized access to IT systems to steal data, disrupt system services or damage IT networks in any way. Ransomware is a type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided. Phishing is an online scam enticing users to share private information using deceitful or misleading tactics.
- **Incident Detection, Response, and Prevention -** Cyber incidents are capable of demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Because of this risk, all organizations and even individuals should have clear, executable cyber incident detection, response, and prevention strategies. Cyberattacks are evolving and becoming increasingly complex and hard to detect.
- **Information Sharing -** Information sharing is essential to furthering cybersecurity for the Nation. Isolating cyberattacks and preventing them in the future requires the coordination of many groups and organizations. By rapidly sharing critical information about attacks and vulnerabilities, the scope and magnitude of cyber events can be decreased. With the right plans, processes, and connections in place, information sharing can be a seamless step of cyber incident response procedures and a first defense against wide-spread cyberattacks.
- **Securing Networks -** The federal enterprise depends on information technology (IT) systems and computer networks for essential operations. Keeping networks safe protects the vital information and operational processes that live and depend on these systems. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems. Securing a network involves continuous monitoring, assessments, and mitigation across various interrelated components, including servers, the cloud, Internet of Things (IoT), internet connections and the many physical assets used to access networks.
- **Advanced Persistent Threats -** An advanced persistent threat (APT) is a well-resourced adversary engaged in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion. APT objectives could include espionage, data theft, and network/system disruption or destruction. According to National Institute of Standards & Technology (NIST), an APT is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

A strategy and a future implementation plan will help the federal government address four major cybersecurity challenges:

1. **Establish and implement a comprehensive cybersecurity strategy and perform effective oversight.** The strategy articulates goals and strategic objectives for a more coordinated approach to address the Nation's cybersecurity challenges.
2. **Secure federal systems and information.** The strategy identifies steps and priorities to mitigate cybersecurity risks in federal systems.
3. **Protect cyber critical infrastructure.** The strategy identifies investment priorities to defend critical infrastructure against cyber threats.
4. **Protect privacy and sensitive data.** The strategy identifies the need for increased investments in privacy preserving technology.

DoD Policy Changes & Funding

In response to increased cybersecurity concerns and threats across the world, cyber policies have been updated and the U.S. (DoD) has introduced the (CMMC) requirement for federal contractors. The U.S. Federal government has updated mandated policies under Federal Acquisition Regulation (FAR) contract clauses through the CMMC program for Federal contractors to become compliant. As a result, there is a looming sense of pressure to ensure all Federal contractors are compliant to continue smooth operations running smoothly.

The continuing aging of infrastructure and climate challenges concerns makes it more challenging but necessary to ensure a clean energy future that addresses consumer expectations and behavior. The U.S. Federal Government continues to transform itself including decarbonization, electrification, digitization resulting in new federal funding opportunities which all consist of various cyber threats and potential concerns to cybersecurity. Additionally, Governments, businesses, and utilities have set ambitious sustainability goals which require cybersecurity considerations.

As a result, in the past couple of years, Washington has delivered on the biggest federal investment in infrastructure in decades, including more than $62 billion for electric and grid networks and more than $47 billion for resilience — including cybersecurity — as part of the $1.2-trillion Infrastructure Investment and Jobs Act (IIJA). Government agencies, federal contractors and stakeholders must move fast enough to meet these demands to ensure a secure and resilient future.

More recently, the DoD released its new 2023 Cyber Strategy and will pursue four lines of effort to:

Defend the Nation – Work to determine cyber threats; disrupt and degrade malicious cyber actors' capabilities; work with interagency partners to defend U.S. critical infrastructure (including the U.S. Defense Industrial Base (DIB) and counter threats to military readiness

Prepare to Fight and Win the Nation's Wars – Ensure the cybersecurity and defense of the Department of Defense Information Network (DODIN); enhance the cyber resilience of the Joint Force to fight in and through contested cyberspace; and use cyberspace to meet the Joint Force's requirements and generate asymmetric advantages

Protect the Cyber Domain with Allies and Partners – Build the capacity and capability of U.S. Allies and partners in cyberspace and expand cyber cooperation while encouraging adherence to international law and internationally recognized cyberspace norms

Build Enduring Advantages in Cyberspace – Optimize the organizing, training, and equipping of the Cyberspace Operations Forces and Service-retained cyber forces; ensure the availability of timely and actionable intelligence; explore emerging technologies for cyber capabilities; and foster a culture of cybersecurity and cyber awareness across the DoD through education, training, and knowledge development

Federal funding will support the millions of electric vehicles (EVs) entering service and provide a significant business opportunity to a market that experienced years of flat load growth is not lost on industry stakeholders. Similarly, awareness of the critical role energy storage will play in providing grid-balancing support comes as the pace of renewable energy deployment accelerates. Grid resilience to climate impacts, cybersecurity and a series of interconnected elements round out a range of choices reflecting the competing priorities within the broader grid modernization effort.

Secure, Resilient & Sustainable Infrastructure

Never has the U.S. Federal Government faced stringent requirements to become resilient and reliable which has a significant impact to potential cybersecurity threats. From rapidly increasing load demand attributed to fleet electrification and the buildout of electric vehicle (EV) infrastructure to the stresses of climate change and issues involving intermittencies of renewable energy, the robustness of the Nation's infrastructure and energy system is under scrutiny. Incentivizing the energy transition for the military will either require new infrastructure or upgrades, mods, or renovations to existing infrastructure to meet the global impacts of governments accelerating demand for clean technology (e.g., IIJA and other federal funding):

- Grid Modernization and the Grid Edge
- Decarbonization & Zero-Emission Sustainability Goals
- Electrified Transportation/Fleets
- Climate Change

Keyboard troublemakers hellbent on exploiting network vulnerabilities to inflict grid-disrupting damage are an unrelenting handful for cyber professionals. In January, **Utility Dive reported** that FERC is considering developing new cybersecurity rules for DERs on the bulk electric system, and the Department of Energy is funding "next-generation" cybersecurity research, development and demonstration projects. Also, clients are facing outflows of experienced professionals and need help running their facilities and assets efficiently. This, coupled with the need to modify or upgrade to meet decarb and sustainability goals, is an increasingly important need.

Black & Veatch's mission is to help the U.S. Federal Government to implement defenses against the leading cyberattack vectors in order to reduce their risk of data breaches and other disruptive and damaging cyberattacks. When climate change and natural disasters occur this can cause disruptions and threats to our Nation's critical infrastructure impacting cybersecurity concerns. Black & Veatch experts are committed to continue leading cybersecurity solutions for U.S. Federal Government to:

- Apply world-class capabilities to ensure the highest possible level of cyber, physical, and electronic security on programs of critical national interest to numerous government agencies.
- Provide design solutions of U.S. Government facilities including network protection design, BAS control protection, and data center protection supporting the Cyber warfighter mission.
- Deliver end-to-end solutions including consulting, security, site-selection & assessment, planning, engineering & design, project management & construction services and operations and management.

Cybersecurity Maturity Model Certification (CMMC) 2.0

To safeguard sensitive national security information, the DoD launched CMMC 2.0, a comprehensive framework to protect the defense industrial base's (DIB) sensitive unclassified information from frequent and increasingly complex cyberattacks. The CMMC 2.0 program is the next iteration of the CMMC cybersecurity model. It streamlines requirements to three levels of cybersecurity and aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards. With its streamlined requirements, CMMC 2.0:

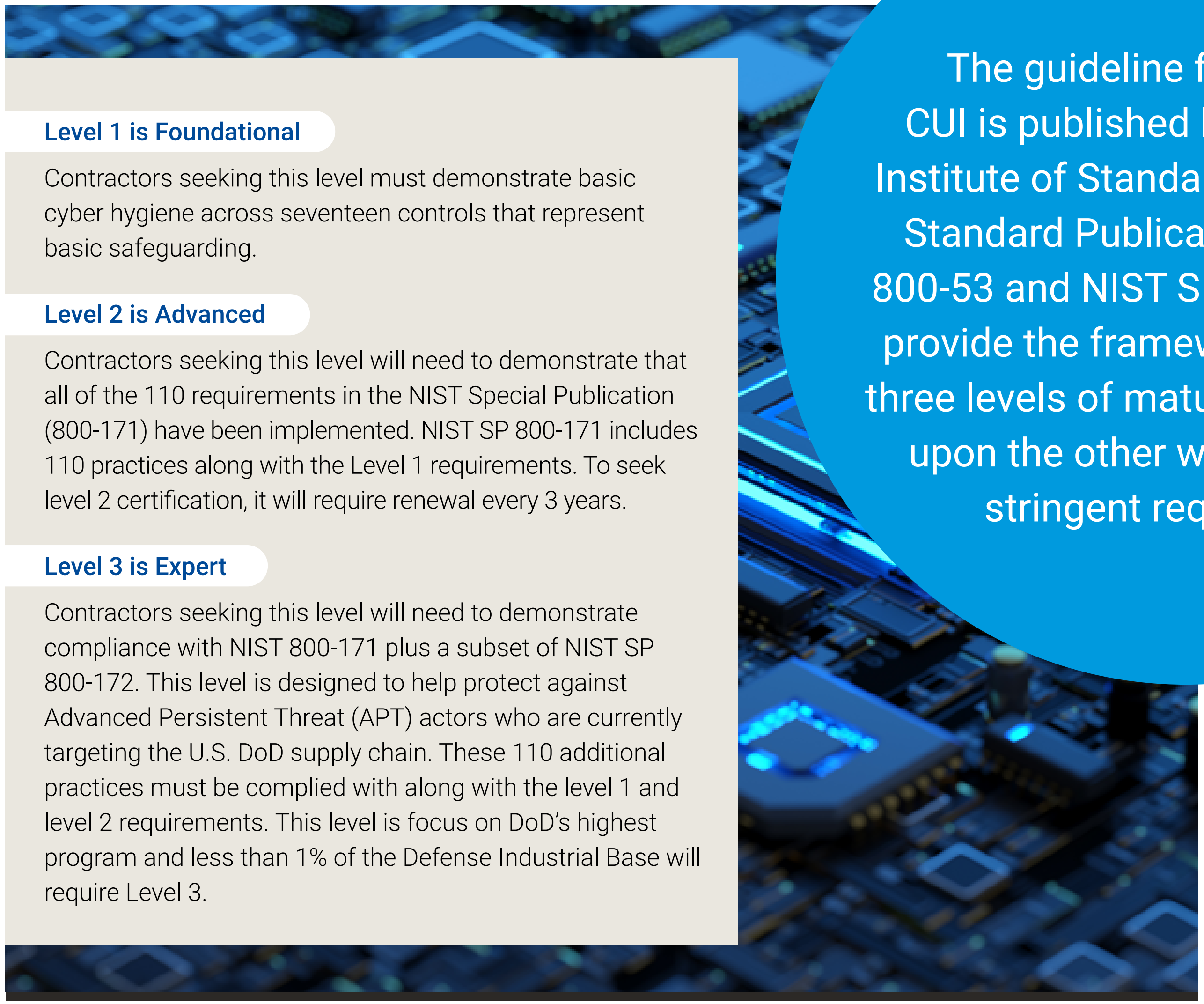
- Simplifies compliance by allowing self-assessment for some requirements
- Applies priorities for protecting DoD information
- Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

The Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 requires contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network.

The CMMC framework is the result of the following philosophical change to how the Nation's data is secured:

- Increased expectations for accountability and integrity about cybersecurity
- Transparency between traditionally isolated entities required a shift from trusting contractor's self-attestations and plans of action to fix gaps to requiring an independent on-site validation of full compliance.
- Changed expectations for IT Teams
- Need to understand the information flow to know how to protect the information
- This also required a shift from a "protect the system" mindset to a "protect the information" mindset

This change introduced the independent Certified Third-party Provider Assessment Organization (C3PAO). This organization is responsible for verifying the contractor's compliance. The CMMC Accreditation Body is authorized by the US Department of Defense to be the sole authoritative source for the operation of CMMC Assessments and Training with the DoD contractor community, or other communities that may adopt the CMMC. It does not endorse, support, or promote any organization outside of the Accreditation Body that might use the acronym "CMMC" in their organization name, or in any description of the services they may provide.



Level 1 is Foundational

Contractors seeking this level must demonstrate basic cyber hygiene across seventeen controls that represent basic safeguarding.

Level 2 is Advanced

Contractors seeking this level will need to demonstrate that all of the 110 requirements in the NIST Special Publication (800-171) have been implemented. NIST SP 800-171 includes 110 practices along with the Level 1 requirements. To seek level 2 certification, it will require renewal every 3 years.

Level 3 is Expert

Contractors seeking this level will need to demonstrate compliance with NIST 800-171 plus a subset of NIST SP 800-172. This level is designed to help protect against Advanced Persistent Threat (APT) actors who are currently targeting the U.S. DoD supply chain. These 110 additional practices must be complied with along with the level 1 and level 2 requirements. This level is focus on DoD's highest program and less than 1% of the Defense Industrial Base will require Level 3.

The guideline for protecting CUI is published by The National Institute of Standards & Technology Standard Publications (NIST) SP 800-53 and NIST SP 800-171. These provide the framework for CMMC's three levels of maturity each building upon the other with increasingly stringent requirements.

PATH FORWARD

Five Steps to Become More Cyber Secure

(according to DoD for CMMC 2.0 Implementation)

1.

Educate people on cyber threats
Most cyber incidents start because of user error. Educate people about the importance of setting strong passwords, recognizing malicious links, and installing the latest security patches.

2.

Implement access controls
Limit information systems access to authorized users and the specific actions that they need to perform.

3.

Authenticate users
Use multi-factor authentication tools to verify the identities of users, processes, and devices.

4.

Monitor your physical space
Escort visitors and monitor visitor activity, maintain audit logs, and manage physical devices like USB keys.

5.

Update security protections
Automate testing and application of the latest security patches when new releases are available. Always double check to make sure they are coming from a trusted source.

Stakeholder Engagement with Utilities

Like with any U.S. Federal contract, Federal contractors are required to engage with critical stakeholders throughout the duration of the project — such as multiple government agencies sometimes varying across different branches, power utilities, water utilities, technology vendors, rural communities, and higher education entities. This impacts decision making and requires addressing cyber concerns and potential threats particularly when engaging with utilities that provide energy and water sources critical to the government's mission.

Water Utilities

When it comes to safeguarding water utilities, cybersecurity is top of mind. The U.S. water sector gets it, overwhelmingly demonstrating great awareness about the importance of and need for cybersecurity postures as they harden their systems against such attacks. The big takeaway: Eight in ten of our survey respondents report that cybersecurity is the most important investment in the security of their assets. But only 57 percent believe physical security — a prerequisite for cybersecurity — is the most critical investment. That gap could jeopardize both.

> "The vast majority of treatment costs will be borne by communities and ratepayers, who are also facing increased costs to address other needs, such as replacing lead service lines, upgrading cybersecurity, replacing aging infrastructure and assuring sustainable water supplies."
>
> - AMERICAN WATER WORKS ASSOCIATION

Network security threats are a very real challenge for water utilities. Cybersecurity comes at a cost around valuing and investing in smart technology but also safety and security. When they occur, cyberattacks not only erode customer confidence and cost money, they compromise the ability to provide clean, safe drinking water or effective wastewater management to communities. A breach of your systems is a breach on your community's resilience and customer confidence in the utility to provide the services promised. That changes the age-old question of "Can I really afford it?" to "Can I really afford not to have it?"

The proliferation of even more standards and regulations in recent times has made simply navigating the relevant cybersecurity standards and guidance a daunting task. With a solid background and understanding of these regulations, Black & Veatch can audit the SCADA system to determine the areas of highest vulnerability — helping you understand where best to start.

Cybersecurity breaches can lead to:

- Defacement of the utility's website or compromise of the email system.
- Theft of customers' personal information from billing systems.
- Redirection of financial payments to malevolent individuals or groups.
- Release of ransomware that can disable maintenance, customer service and billing.

Even worse, cyberattacks on water, wastewater, or stormwater utilities' industrial control systems, called SCADA systems or operational technology (OT), can cause significant harm through alterations in the treatment or conveyance processes. These can include:

- Releasing ransomware that mandates manual control.
- Changing chemical dosing that could injure people or mandate boil water alerts.
- Opening and closing valves or stopping pumps that could prevent firefighting.

Older, simpler water systems are open to purposeful, malicious disruptions, from supply contamination to cyberattacks potentially damaging and risking the public health of the communities. In Black & Veatch's recent Water Report found that U.S. water utilities are prioritizing investments — whether supported by new funding programs or not — 50% responded that cybersecurity is one of their top investments for their utility or municipality over the next decade. Cybersecurity was the top issue among respondents that had studied their vulnerability, and it is the third highest area where all respondents expect to see major investment.

In March 2023, the U.S. Environmental Protection Agency (EPA) announced a new plan to improve the digital defenses of public water systems, with the EPA's assistant administrator for water putting the gravity of the issue in clear but stark terms. "Cyberattacks against critical infrastructure facilities, including drinking water systems, are increasing, and public water systems are vulnerable," Radhika Fox, in EPA's official announcement.

> "Cyberattacks have the potential to contaminate drinking water, which threatens public health."

That recent warning involving an industry where there's no one-size-fits-all approach to addressing vulnerabilities in operations and assets offers a backdrop to today's conversation about cybersecurity in Black & Veatch's 2023 Water Report, based on survey responses from 450 U.S. water sector stakeholders.

Among the key findings: utilities overwhelmingly demonstrate great awareness about the importance of and need for cybersecurity as they continue to make progress in hardening their systems against such attacks. Eight in ten respondents reported that cybersecurity is the most important investment in the security of their assets. While that's certainly positive, only 57 percent believe physical security — a prerequisite for cybersecurity — is the most critical investment.

A More Holistic Approach

That gap in prioritization may result in vulnerabilities in one — or both — of these areas. While it is encouraging that such a high percentage of respondents are addressing the need for strong — or stronger — cybersecurity practices, there's opportunity for more collaboration among cybersecurity and physical security professionals to take a more holistic approach to their security programs.

The report showed utilities prefer to be trusted to go it alone with their cybersecurity without governmental oversight. Seven in ten respondents (72 percent), when asked if they would prefer cybersecurity to be regulated and have a compliance standard or prefer it to be self-governed by the utility, chose the route of independence. Given the high cost of complying with federal regulations observed in other sectors — as well as competing needs for limited utility funds — utilities simply may see a cost benefit in managing cybersecurity without federal oversight, regardless of the security implications that may result.

That is not to say they do not desire or enlist outside help; nearly 80 percent of respondents say they have hired or consulted with cybersecurity experts or information security engineers — whether it is having full time staff, consulting with external experts, or hiring on a part time or contract basis.

The bottom line, according to Black & Veatch's survey: utilities have strong efforts in place to mitigate against today's biggest security threats. While competing interests and limited resources create even more headwinds, U.S. water utilities have the foundation — and no shortage of expert consultants such as Black & Veatch to help them navigate complexities — to continue building strong, robust cybersecurity programs to protect such undeniably critical human infrastructure.

Power Utilities

With the relentless surge of renewables, how do U.S. electric utilities find ways to integrate it all onto the grid — a task that our survey of about 250 power sector stakeholders cite for the second consecutive year as their top challenge, along with aging infrastructure?

Funding from the IIJA, also known as the Bipartisan Infrastructure Law and signed into law in November 2021, certainly helped impact at least some of this investment decision-making by virtue of the $107 billion it will provide in funding and incentives for clean energy, power, and electricity grid reliability projects. The more recently enacted IRA — approved by Congress and signed into law in August — provides another $369 billion in funding incentives for clean energy, arguably making it the most impactful piece of energy policy ever enacted in the United States.

The **Black & Veatch 2022-2023 Electric Report** — based on survey data from roughly 250 U.S. electric sector stakeholders — the report says Cybersecurity ranked sixth in 2020 before rising to second last year, then fell to eighth this year at 18 percent, giving way to tightly grouped concerns about reliability (21 percent) and planning and forecasting uncertainty (19 percent).

The goal is to reduce carbon emissions by 40 percent by 2030, however current investment in electric infrastructure to get there still does not match the need.

Because of the highly dynamic technology and threat environment, cybersecurity has its tentacles in nearly every aspect of the electric industry, from assessing ongoing threats to identifying and mitigating system vulnerabilities, commissioning new devices that monitor air quality, and securing weather stations. As if that were not enough, cybersecurity experts in the electric sphere are responsible for maintaining compliance with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards.

Long story short, the industry's cybersecurity professionals have their hands full. But Black & Veatch's 2022-2023 Electric Report illustrates that these professionals are rising to the occasion, performing regular cybersecurity assessments, showing awareness of the latest threats, and exploring new technologies and platforms to modernize their organizations.

Invisible. **Invaluable.**

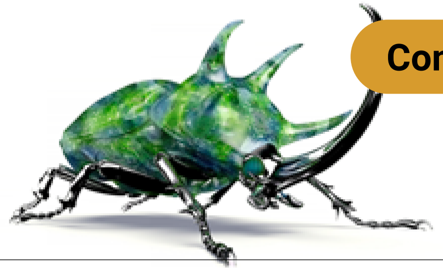
Critical mission infrastructure is more than facilities and programs you can see, it is the strategic detection and deterrence of any threat. At Black & Veatch, our mission is to provide competitive advantages for clients seeking to protect our Nation, eliminate threats, and strengthen its systems so they work no matter what. Ensure resilience in your facility, infrastructure, or program to eliminate cyber threats. Let's Talk.

Learn more about Black & Veatch's cybersecurity expertise and connect with us about your reliability and resilience goals.

10 Steps to Deploy Military Electric Fleets
Optimal Charging Networks for Reliability, Resilience, and Sustainability
BLACK & VEATCH
2023 Water Report
2023 Electric Report

Read our other eBooks and Reports to stay resilient and secure from threats

How CyberSecure is your infrastructure?



Contact us