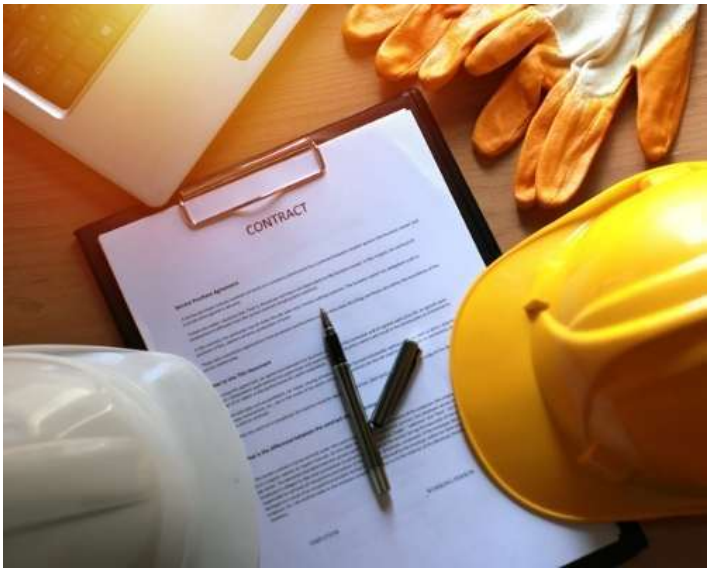
Viewpoint Blog

8 Major Cybersecurity Requirements Contractors Need to Bid for Government Contracts



Contractors need to ensure high cybersecurity standard to net today's government contracts.

State and local governments spend more than $250 billion every year constructing roads, bridges, rail lines, utilities, schools and other public infrastructure … and that's *before* the 2021 infrastructure bill, which could usher in an additional $1.2 trillion in spending for construction projects.

The comprehensive infrastructure bill is bringing government contracts into the headlines today; but federal, state and local projects have always been a good way for construction contractors to maintain a steady source of revenue.

What's new are the complex technology and cybersecurity requirements that companies must follow to play the game.

What Are Cybersecurity Frameworks? (& Why Should You Care)

Having the right cybersecurity measures in place can provide a leg up in winning new work.

Frameworks are a system of standards, guidelines and requirements that help companies avoid cyber risks and keep data secure. There are several different frameworks which address risk, cybersecurity programs, and/or security controls and implementation.

Different cybersecurity frameworks are appropriate for different ways of doing business, and different company goals. Some frameworks may be a compliance requirement of a governing body or a vendor contract, while others are voluntary and might prove good environmental risk management to investors.

But if your business is done with a handshake, why should you care about data and security? Well, regulatory compliance is in your own best interest. Cybersecurity guidelines:

1. crack open massive government construction opportunities
2. keep company and customer data safe from hackers and data breaches
3. modernize and secure your assets against risk and business disruption
4. make your business more attractive and competitive

We asked cybersecurity expert Bryce Austin to break it down for construction contractors who want to modernize their business and be eligible to bid on government contracts.

What are the Most Common Cybersecurity Frameworks?

There are a number of cybersecurity frameworks and standards applicable to businesses today.

You may have already heard of the most common cybersecurity frameworks. These include:

- **NIST (US National Institute of Standards and Technology)** addresses cyber risks and is considered the gold standard of cybersecurity regulations
- **SOC II Type 2** enables organizations to obtain a certification of compliance
- **ISO (International Standards Organization)** frameworks, especially ISO 27001 and 27002, are international standards of security validation
- **NERC-SIP** is focused on third-party risk in the utility and power grid sector

For contractors of federal agencies, the NIST Cybersecurity Framework is required. That

makes NIST 800-171, along with SOC II Type 2, the place to start.

What is NIST 800-171 — and How to Get Started?

Good old NIST, which helps businesses create risk management controls for their information security program, has been updated a few times since its establishment in 1901. Specifically, NIST 800-171 addresses cybersecurity and shows how contractors and subcontractors of Federal agencies should manage Controlled Unclassified Information (CUI).

NIST 800-171 is designed specifically for non-federal organizations. It is based on DFARS, an earlier cybersecurity framework that was created for defense contractors.

NIST is a good framework, according to cybersecurity expert Bryce Austin, because "regulatory compliance is in your own best interest. You don't want to get ransomware, and the government also doesn't want you to get ransomware. It's a win-win." You'll want SOC II Type 2 as well, Austin adds.

8 Top Cybersecurity Requirements for Government Contractors

Safeguards like Multi-factor Authentication can help reduce chances that cybercriminals can gain access to your data.

1. Multi-factor Authentication (MFA)

MFA includes three aspects: something *you know* (like a password), something *you have* (like a smartphone or device), and something *you are* (like a fingerprint, or a face or retinal scan). MFA must include any two of these three factors.

“It will keep out 99% of bad guys. NIST demands it, and before that DFARS demanded it,” Austin says. LogMeIn, Okta, Duo are some of the biggest MFA services.

2. Good Password Controls

Your employees’ passwords can’t be junk, or include obvious substitutions — that means no “Pa$$w0rd”, “summer2021”, or dates based on your birthday.

And don’t use the same password for all of your accounts, Austin adds. It’s an unfortunate fact that most adult Americans have had their data stolen more than once. If a long-forgotten account was hacked (it probably was), any other accounts with the same password are compromised. “This is particularly true for employees at the executive level,” he notes.

Strong password requirements have also helped significantly thwart security risks.

3. Educate Executives

Executives should get ongoing security education that is a step beyond normal users, because they’re a much richer target. Executives have access to financial information and sensitive data at the highest levels of the company.

4. Deprecate Old Systems

Have an end-of-life plan to deprecate old systems, which could be supporting employees’ connected smart devices or running other critical operations. “Your Windows 2007 and 2008,” Austin says, “should be GONE!”

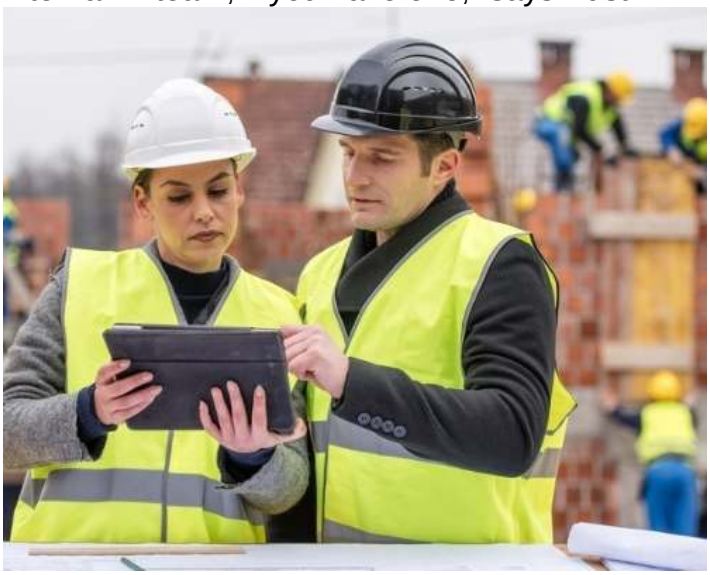
Austin recommends looking for "next-gen firewall features" that can detect abnormal digital traffic patterns.

5. Establish Perimeter Firewalls

Austin suggests looking for “next-gen firewall features” — technology that looks for deviations in normal website traffic behavior. However, Austin says, “It’s a common misconception that if you have a firewall, you don’t have to worry about cybersecurity threats. Not true. They’re a huge factor of good cybersecurity, but firewalls alone are not enough.”

6. Antivirus and Endpoint Protection

Endpoint protection keeps data secure on individual devices. Construction contractors should have end-point protection *everywhere*: every laptop, every server, every mobile device. Some companies offer a “security as a service” model, where their own response team helps in case of a security event. “It’s a good checks and balances measure for your managed service provider or internal IT team, if you have one,” says Austin.



Controlling end-users permissions or access to data is a key strategy to protecting sensitive information.

7. Role-Based Access Controls

Not everyone who interacts with your company needs to access the same information. With role-based permissions and other access controls, users are assigned to roles, and each role is assigned one or more privileges that are permitted to users in that role.

8. Internal Penetration Tests and Vulnerability Scans

Perform regular penetration tests and look for chains of vulnerability that could lead to a big hack. “Assume a user clicked a bad link,” Austin suggests, “and follow that path to see what a bad guy can do with that.”

Additionally, monthly vulnerability scans can tell you a lot about the care and feeding of your network.

A Case for Moving to the Cloud

Implementing the NIST 800-171 framework is a big job. It will take more than one person to do it … and it might change the way you do business, says Austin. You may need to change your hardware requirements, for example. But in order to do business under stringent governmental regulations and guidelines, they're necessary actions.

That's why many contractors today are scaling their operations by moving to hosted cloud construction and business management solutions that have many of these cybersecurity protections built in.

Real-Life Story

Watch this video to see how a ransomware attack impacted contractor E.R. Snell and how it responded.

Posted By

Charity Heller

Charity Heller leads the Viewpoint content team. She is passionate about engaging new audiences and creating relationships through storytelling, data, strategy, and inclusion.