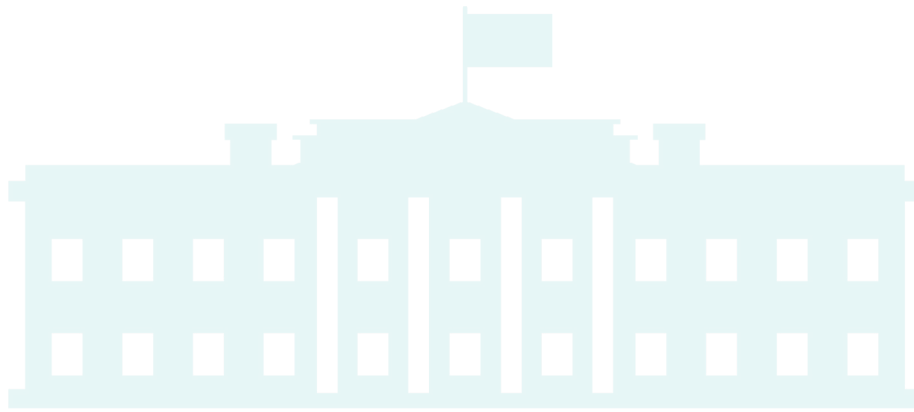


The Preparation Guide

for the **White House** Cybersecurity
Recommendations for **Software Development**



Overview.....	1
Overview of White House Statement and Fact Sheet of March 21, 2022.....	2
How the New Regulations Impact Software Providers.....	4
Resources and Best Practices for Organizational Cyberdefense Readiness.....	5
Solutions for Cybersafety in Your Work and Life.....	8
How Kiuwan Can Help You Comply with Cybersecurity Requirements.....	9



On April 4, 2022, the State Department formed a new bureau, the [Bureau of Cybersecurity and Digital Policy](#) (CDP). The establishment of the new bureau should come as no surprise since the White House released a [statement](#) on March 21, 2022, urging the federal government's private sector partners to:

"...harden your cyber defenses immediately by implementing best practices we have developed together over the past year." The Biden administration also released a [fact sheet](#) the same day entitled, "Act Now to Protect Against Potential Cyberattacks."

Furthermore, the administration mandates extensive cybersecurity measures for the federal government and any critical infrastructure where it has the authority to do so, including the software supply chain.

The statement and the fact sheet refer to the [Executive Order](#) on Improving the Nation's Cybersecurity that the President of the United States signed on May 12, 2021.

What do these three documents mean for you and your software development business? We offer you this preparation guide for the White House cybersecurity recommendations to clarify and simplify your efforts to comply with not only the cybersecurity requirements of the federal government but also to help you meet standards already in place and position your organization for future standards compliance.

Since the federal government already uses a multitude of software and cloud products and services provided by the private sector, your company may already be considered a government contractor or supplier. Cyberattacks were already on the rise when recent political events shone a bright spotlight on potential infrastructure weaknesses exploitable by bad actors.

This preparation guide provides you with a roadmap to compliance and security for your organization and your external users.



Overview: *White House Statement* and Fact Sheet of **March 21, 2022**

The White House statement reiterates warnings about the potential for malicious Russian cyber activity against the U.S. in answer to deepening sanctions. The intelligence agencies suggest the Russian government is exploring other cyberattack options as well.

The federal government must actively work with private sector infrastructure owners and operators to quickly identify and block cyberattacks.

According to the White House statement, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) actively works with organizations across the national infrastructure to rapidly share information and mitigation guidance. The department expects its guidance to help protect networks and systems.

As mentioned above, it also urges private sector partners to harden their defenses immediately if they have not already done so.

The fact sheet contains a list of required steps for organizations working on federal contracts to become compliant and continue as federal contractors.

- ☒ **Mandate multi-factor authentication (MFA).**
- ☒ **Deploy security tools to continuously monitor, identify, and mitigate threats.**
- ☒ **Patch and protect systems against all known vulnerabilities.**
- ☒ **Back up data and ensure offline backups are out of the reach of bad actors.**
- ☒ **Run exercises and drill on emergency plans so staff can respond quickly to minimize an attack's impact.**
- ☒ **Encrypt data to prevent use if stolen.**
- ☒ **Educate employees on common cyberattack tactics.**
- ☒ **Engage proactively with the local CISA or FBI regional office to establish a relationship ahead of potential incidents or events.**



To harden systems against known vulnerabilities, mandate password changes across the network to remove the threat posed by stolen credentials. Employees should understand that cyberattacks can begin with an email or website link.

If any computer or mobile device shows unusual behavior, such as frequent crashes or slow operations, the user should report the issue to your information technology (I.T.) and cybersecurity teams.

A Note about *Open-Source* Software

Software developers make frequent use of open-source software and third-party code in almost all projects. While the industry has hailed open-source software as an efficient step forward in programming, it also poses dangers.

According to the latest report from the Open Web Application Security Project (OWASP), the top ten web application security risks in 2021 were as follows, in decreasing order of occurrence. Most risks appeared on the 2017 list but may have moved up or down the list in the past few years.

1. Broken access control
2. Cryptographic failures
3. Injection events
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery



Developers should use the OWASP Top Ten to ensure they use secure coding practices and open-source software versions.



How the *New Regulations Impact Software Providers*

While most of the notification and information-sharing provisions focus on federal contractors, many of the same software products used in the private sector are also used by the federal government and its departments and agencies.

In addition to the statement and fact sheet released this past March, the White House issued an [Executive Order](#) in February 2021 that directs the National Institute of Standards and Technology (NIST) to develop guidelines for secure software development that all commercial suppliers to the government must follow. The guidelines will probably become standards in the future for voluntary adoption.

Government software vendors number in the [hundreds of companies](#), including:



Many, if not most, software developers potentially use one software development process across the organization and products. All private-sector users benefit from security enhancements performed at the behest of the federal government.

The Executive Order on America's Supply Chains [requires all](#) federal contractors to use MFA, encrypt data, and use administratively separate build environments for each product.



In addition, it requires vendors to maintain a vulnerability disclosure program to make the results of automated security checks public and provide a software bill of materials (SBOM) listing all software and sources used in the development of the product.

Indirect Impacts on Private Sector Companies

Not all provisions directly affect software providers; many of the impacts are indirect but beneficial to the private sector and the government.



For example, cloud services providers are incentivized to provide highly secure services and provide both private customers and the federal government more control over the use of the service.

Also, world events continue to level within 36 hours after the bank determines an incident occurred. It also requires providers to notify each affected bank organization as soon as possible after identifying an incident.

The Executive Order on Improving the Nation's Cybersecurity, signed May 12, 2021, affects data breach reporting requirements for Information Technology (I.T.), Operational Technology (O.T.), and Information and Communication Technology (ICT) service providers.



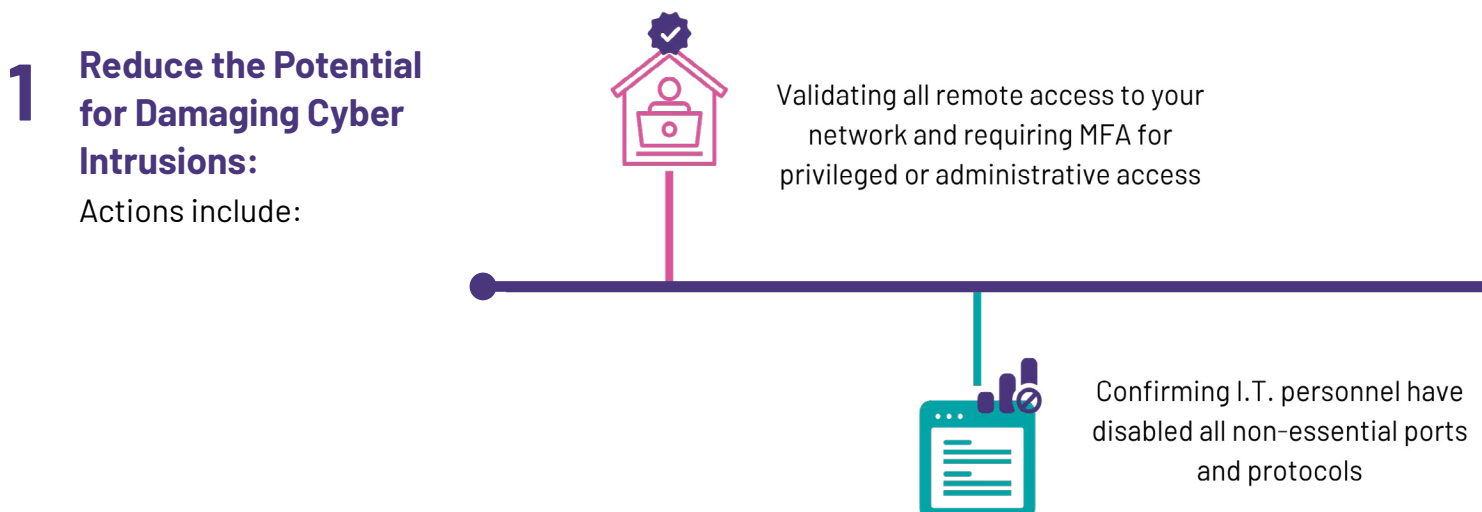
Resources and Best Practices for Organizational Cyberdefense Readiness

The CISA launched a significant resource for businesses called the Shields Up campaign. It addresses intelligence that Russia has the potential and incentive for malicious software activity and provides a series of recommendations to help you *"prepare for, respond to, and mitigate the impact of cyberattacks."*

The campaign recommends that all organizations, regardless of size, adopt what it calls a heightened security posture to protect critical assets. Shields Up also provides free cybersecurity tools and services from government partners and industry.

Recommendations from the Shields Up Campaign

The Shields Up campaign provides a series of recommendations.





Updating software and prioritizing updates addressing known exploits and vulnerabilities identified by the CISA



Signing up for free cyber-hygiene services through CISA, including vulnerability scanning, to reduce your threat exposure



Reviewing and implementing strong controls if your organization uses cloud services as outlined in the CISA guidance

2 Prepare To Detect Potential Intrusion Quickly

Actions include:

- ☐ Focusing your I.T. team on identifying and quickly assessing any unexpected or unusual network behavior and enabling logging to investigate events or issues better.
- ☐ Confirming your company's entire network is protected by anti-virus and anti-malware software, including updated signatures in the tools.
- ☐ Using additional caution when working with Ukrainian organizations by monitoring, inspecting, and isolating traffic from those organizations.
- ☐ Closely reviewing access controls for Ukrainian traffic.

3 Prepare To Respond if an Intrusion Occurs



Actions include:

- ☐ Designating a crisis response team with the main points of contact for suspected cybersecurity incidents, roles and responsibilities, and continuity planning for technical, communications, and legal services.
- ☐ Ensuring availability of key personnel and identifying a means of surge support for responses.
- ☐ Conducting tabletop exercises with all participants to ensure they understand their roles in the event of an incident.



4 Maximize Your Organization's Resilience to Cyberattacks

Actions include:

-  Testing all backups to determine if critical data is rapidly restored after a ransomware event or cyberattack.
-  Conducting tests of manual controls if using industrial automation control systems to ensure critical functions are operable if your network becomes untrustworthy or unavailable.

Review the CISA Publication Entitled Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

After reviewing this publication, visit [StopRansomware.gov](https://www.stopransomware.gov) to obtain further resources and sign up for alerts.

*The tools and resources from the [Shields Up Campaign](#) are already available to all organizations.

Best Practices

The federal government encourages you to follow these best practices for secure software development, deployment, and management decision-making. The **best practices** are as follows:



Build security into your software. Don't try to retrofit security or bolt it on after development is complete.



Use highly secure environments accessible only to those who must have access to prevent an intruder from jumping from system to system and compromising or stealing your intellectual property (I.P.).



Use automated tools to check for known and potential vulnerabilities and find the most coding errors before the software ships.



Ensure your **developers know the provenance of all software used in a project** and include a software bill of materials (SBOM), checking the origin of the code and tracking all security updates to that code.



Empower your **chief information security officers (CISOs)** by including them in the **decision-making process around risks** to the company. Ensure everyone in the organization understands that investing in security is an immediate top priority.





Lower your documented reporting thresholds for potential cyber incidents so that senior management and the U.S. government remain informed. Senior management must establish the expectation that any indications of cybersecurity issues are reported to Report@CISA.gov, even if security controls block them.



Participate in a test of your response plans. Include the security and I.T. teams, the senior business leaders, and all members of your board of directors. Have everyone perform tabletop drills to ensure familiarity with how you manage these events for your company and within your supply chain.



Focus on continuity. Recognize your finite resources and invest in security and resilience. Ensure you target systems supporting critical business functions and have senior management identify and continually test continuity planning to ensure all functions are available after a cyber event.

The final recommendation from the Shields Up campaign is to prepare for the worst. There is no credible information about specific threats to the U.S., but the federal government encourages everyone to plan for a worst-case scenario.

Senior management should use robust procedures and measures to protect your most critical assets in case of intrusion. Include the disconnection of high-impact parts of your network as part of your plan.


Solutions for Cybersafety in Your Work and Life

The best solution for avoiding cyberattacks is to think before you click. Over 90% of all cyberattacks begin with a phishing email with a legitimate-looking link to a website.

Once clicked, malware targets passwords, social security numbers, credit card numbers, or other sensitive information. Everyone in your organization should learn to identify and report suspicious email links.

Make sure you and your employees use strong passwords. The easiest way for everyone to control their passwords and change them regularly is by using a password manager, and the manager can both store and generate unique passwords.





Update all software used in your organization and turn on automatic updates where practicable. Include updating the operating systems on mobile phones, tablets, and laptops. Update all applications, including the web browser, and leverage all automatic updates.

Require MFA on all accounts with confirmation via *one of the following*:

- Email
- Text
- Authentication code
- Fingerprint or facial ID
- FIDO (Fast Identity Online) key

Finally, use the Joint CISA and Multi-State Information Sharing and Analysis Center ([MS-ISAC](#)) [Ransomware Guide](#) to effectively respond to cyberattacks.

The MS-ISAC steps you through a response process, starting with detection and proceeding through containment and eradication. You learn how to identify impacted systems to isolate them immediately. It recommends shutting down any device that cannot be disconnected from the network, limiting the spread of infection.

Taking a system image and memory capture of a sample of affected devices streamlines the investigation process so you can become operational faster.

The process helps you triage affected systems for restoration and recovery. The MS-ISAC acts as a consultant for your incident response team, helping them develop and document an initial understanding of the attack based on the initial analysis. The group also engages with internal and external teams and stakeholders to determine the best way to help you mitigate, respond to, and recover from a cyber event.

MS-ISAC also recommends consulting law enforcement about available decryptors. Security researchers have already broken the encryption algorithms for some ransomware variants.

How *Kiuwan* Can Help You Comply with Cybersecurity Requirements?

Kiuwan is a code security solution for mobile and web application development. We offer two essential products designed to improve your cybersecurity hygiene.



Our **Code Security - SAST** (static application security testing) tool automatically scans your code to identify and remediate vulnerabilities. Compliant with the most stringent security standards, Kiuwan Code Security covers all important languages and integrates directly with leading DevOps tools across the SDLC.

Our **Software Composition Analysis (SCA)** tool helps you reduce risk from third-party components, remediate vulnerabilities, and ensure license compliance through code scanning and code analysis.



Kiuwan offers further resources to help you harden your infrastructure and securely develop software.

We provide application vulnerability testing, secure software development life cycle (SSDLC), and the ability to identify code injection attacks. Use a holistic cybersecurity approach to all development and operational processes and comply with government regulations.

Kiuwan recommends adopting a continuous security approach by integrating secure development practices throughout the software development lifecycle.

Code injection attacks are some of the most common security flaws in application and software development, but there are ways to prevent and remediate these vulnerabilities in your code.

Kiuwan is your trusted partner in implementing and complying with the White House cybersecurity recommendations. We have a long history of providing tools for successful, secure software development, testing, implementation, and operation. Visit [Kiuwan.com](https://kiuwan.com) for more resources to help you defend your systems against cyberattacks.

YOU KNOW CODE, WE KNOW SECURITY!

GET IN TOUCH:



Headquarters

2950 N Loop Freeway W, Ste 700
Houston, TX 77092, USA



United States **+1 732 895 9870**

Asia-Pacific, Europe, Middle East and
Africa **+44 1628 684407**

contact@kiuwan.com

Partnerships: **partners@kiuwan.com**

