SPRINGBOARD CERTIFICATION

Cyber Standards Check

Continuous Safeguarding of Critical Applications and Data

Are your applications and data safe?

Cyber Standards Check is an application security standards conformance testing tool to ensure the protection of your applications and data.

Cyber Standards Check is:

- **Easy to Use**
- **Continuous**
- **Safe and Secure**
- **Affordable**

Cyber Standards Check is a simple, secure, and affordable application security standard testing tool to help ensure the protection of your applications and data.

Information systems are increasingly susceptible to online attacks, threatening effectiveness and compromising confidential personal or protected data.

> *Globally, **cybercrime was the 2nd most reported crime** in 2016 according to Price Waterhouse Coopers. Cyber-attacks in 2017 happened at nearly **double the rate** of 2016. Could your networks and data be next?*

The shocking reality is that your chances of being hacked are high, and that could come at an enormous cost. According to the latest cyber-security statistics, your business has likely been compromised already and you may not even know it. Organizations have two choices: be hacked and pay an agency to clean up the mess, or proactively safeguard critical applications.

The NIST Risk Management Framework (NIST SP 800-53), Federal Information Security Management Act (FISMA), and Open Web Application Security Project (OWASP) provide comprehensive guidance to help organizations assess and manage risks to their systems and data.

> ***How can you be sure that your application security measures meet or exceed these complex guidelines? Not only that, but can you ensure your security measures conform to these standards on a continuous basis?***

Cyber Standards Check *automates* this process for you, removing any guesswork or human error. Cyber Standards Check is simple to access and use: log in, point to your software code repository, and run. Cyber Standards Check takes it from there, providing continuous, rigorous application source code testing against key cyber security standards and controls.

Cyber Standards Check:

- ✓ Transforms a hard problem to an easy problem in three simple steps: Access, Connect, Scan
- ✓ Continuously scans your code repositories and reports back vulnerabilities via a personalized, secure dashboard
- ✓ Uses multiple scanning technologies, greatly enhancing the speed and effectiveness of conformance testing and application security
- ✓ Enables NIST standard risk and vulnerability identification while your code resides safely in your code repositories – NOT on someone else's system
- ✓ Is available at an affordable price point tailored to your organization

Cyber Standards Check is an offering of the Springboard Testing and Certification Program. Sign up to get more info at https://springboard.nucleaus.com.

Cyber Standards Check is powered NUCLEAUS

Cyber Standards Check
Frequently Asked Questions (FAQs)

What is it? Cyber Standards Check is a simple, secure, and affordable application security standard testing tool to help ensure the protection of your applications and data by monitoring code environments and reporting vulnerabilities. Built with government needs in mind, **Cyber Standards Check** will reduce your risk, save time and save money.

- ✓ Multiple technologies scan repositories providing NIST recommended remediation
- ✓ Provides a single pane of glass for your code repositories/vulnerabilities
- ✓ Simple deployment via virtual solution
- ✓ Provides a time-line of vulnerability remediation status

Why Cyber Standards Check? Cyber Standards Check is designed for companies and developers who want to:

- Implement ongoing transparency and risk management in code repositories
- Proactively and continuously address vulnerabilities in code
- Eliminate critical application security risks

What makes Cyber Standards Check different?

- **Simple. Cyber Standards Check** transforms a hard problem into an easy problem with three simple steps: Access, Connect, Scan.
- **Standards-based. Cyber Standards Check** takes the complexity out of NIST and other application security standards compliance.
- **Secure. Cyber Standards Check** never stores your code providing scan results only you can access.
- **Ongoing. Cyber Standards Check** continuously monitors your code repositories and reports back up-to-date CVE® vulnerabilities via a personalized, secure dashboard.
- **Affordable.** All for a light monthly fee tailored to your organization.

What Standard controls are addressed by Cyber Standards Check? Cyber Standards Check automates vulnerability checking against the NIST Risk Management Framework (NIST SP 800—53 Rev. 4), Federal Information Security Management Act (FISMA), and Open Web Application Security Project (OWASP), providing comprehensive guidance to help organizations assess and manage risks to their systems and data.

Cyber Standards Check

Continuous Safeguarding of Critical Applications and Data

SPRINGBOARD CERTIFICATION

How does Cyber Standards Check work? **Cyber Standards Check** scans code in your GitHub and Bitbucket repositories, providing real-time alerts when new vulnerabilities affect your code. **Cyber Standards Check** works with:

✓ JAVA	✓ PHP	✓ GO	✓ SWIFT
✓ JAVASCRIPT	✓ C++	✓ C	✓ OBJECTIVE-C
✓ PYTHON	✓ C#	✓ SCALA	✓ SHELL & RUBY

**Currently the scanner does not work with PHP or dotNET code base.*

How much time to Deploy Cyber Standards Check? **Cyber Standards Check** is a virtual solution providing a secure virtual appliance for on-premise code scanning, never downloading or copying your code. Once connected, setup can be completed in three simple steps:

1. Download **Cyber Standards Check** Virtual Appliance/Plug-in.
2. Log in to the **Cyber Standards Check** console, register, and add repository and team members.
3. Click *Start* to initiate daily scan(s) and get answers and recommendations.

What kind of access to my repos is required by Cyber Standards Check? **Cyber Standards Check** requires a user account with read-only access to your repositories.

Is my code secure with Cyber Standards Check? Yes. Your code is secure. **Cyber Standards Check** never stores your code – only the metadata is transmitted in an encrypted file. We know your code is extremely important to you and to your business. All private data exchanged with repositories is always transmitted over SSL (which is why your dashboard is provided over HTTPS, for example). All pushing and pulling of private data is done over SSH authenticated with keys, or over HTTPS using your GitHub username and password.

Is your Cyber Standards Check site secure? Yes. Security is at the core of everything we do. We have partnered with Auth0 to create a seamless and secure experience. We have also partnered with SignalSciences for next-gen WAF and RASP solutions.

Will Cyber Standards Check work behind a firewall? Yes. **Cyber Standards Check** is designed to sit on your network behind firewalls.

Cyber Standards Check

Continuous Safeguarding of Critical Applications and Data

SPRINGBOARD CERTIFICATION

What Code Repositories does Cyber Standards Check work with? **Cyber Standards Check** works with BitBucket and GitHub repositories.

What virtual appliances are currently available for Cyber Standards Check? VMWare, Microsoft Hyper-V, and OpenStack are available for use with **Cyber Standards Check**.

Is Cyber Standards Check scan setup configurable? Continuous scans are scheduled every day automatically. A user can opt out of scheduled scans for one, three, five, or seven days.

Will I need to host the Cyber Standards Check dashboard console? No. **Cyber Standards Check** dashboard is a software-as-a-service (SaaS) solution hosted and maintained by **Cyber Standards Check**.

How many team members can I add? Unlimited team members can be added to your repositories.

What happens if I need to actively scan more repositories than I am licensed to scan? If the number of repositories you have exceeds the license type that you have purchased, simply upgrade your license model via the website.

How can I cancel? If you are unsatisfied for any reason, you can cancel at any time via the website.

How can I find out more? **Cyber Standards Check** is an offering from the Springboard Testing and Certification Program. Sign up to get more info at https://springboard.nucleaus.com or contact springboard@ijis.org.

Cyber Standards Check

Continuous Safeguarding of Critical Applications and Data

SPRINGBOARD CERTIFICATION

Cyber Standards Check: Results in Three Easy Steps

1. **Access Cyber Standards Check**.
2. **Connect Cyber Standards Check** to your GitHub or BitBucket software and code repository.
3. **Scan** and see continuous results.

SMALL	MEDIUM	LARGE	X-LARGE	ENTERPRISE
1-2 Repositories	3-10 Repositories	10-50 Repositories	51-100 Repositories	Unlimited Repositories
$100/Month	$200/Month	$500/Month	$800/Month	$1000/Month
One-time setup fee: $100	*One-time setup fee: $200*	*One-time setup fee: $500*	*One-time setup fee: $800*	*One-time setup fee: $5,000*

Cyber Standards Check works with:

- ✓ JAVA
- ✓ JAVASCRIPT
- ✓ PYTHON
- ✓ PHP
- ✓ C++
- ✓ C#
- ✓ GO
- ✓ C
- ✓ SCALA
- ✓ SWIFT
- ✓ OBJECTIVE-C
- ✓ SHELL & RUBY

**Currently the scanner does not work with PHP or dotNET code base.*

Cyber Standards Check

Continuous Safeguarding of Critical Applications and Data

SPRINGBOARD CERTIFICATION