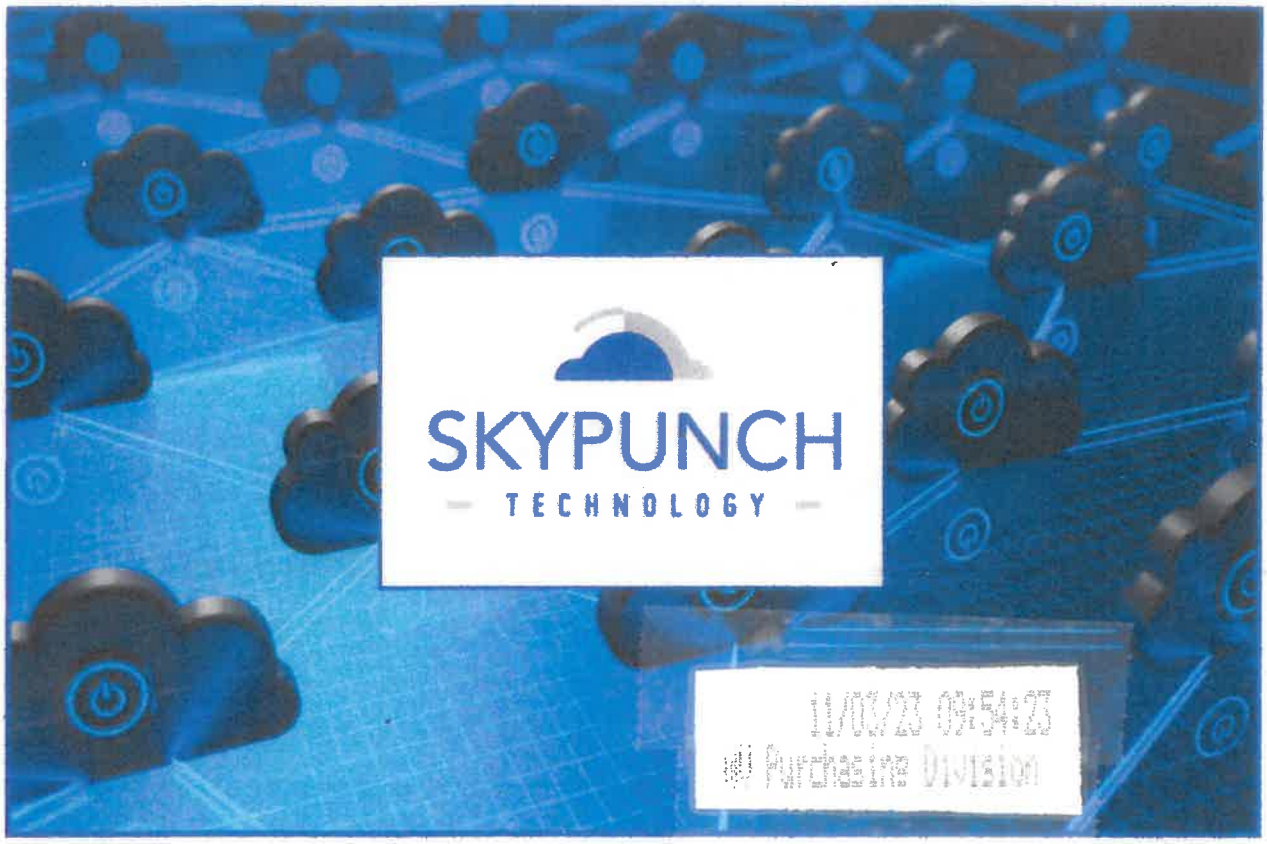


WVSOS Election Division E-ballot Delivery Technology

Technical Proposal

CRFP 1600 SOS2400000001

Skypunch Technology
3803 Staunton Ave SE
Charleston WV 25304

Contact: David Simms
david@skypunch.tech
703-475-6504

www.skypunch.tech

Introduction **1**
History 1
Cryptographic Ballot Verification 1
Cybersecurity **2**
National Institute of Standards and Technology (NIST) Special Publication 800-53 2
StateRAMP 3
Amazon Inspector 3
Amazon Web Services (AWS) Certifications 3
Cybersecurity and Infrastructure Security Agency (CISA) 3
TLS configuration 5
Web Application Firewall (WAF) configuration 5
West Virginia University (WVU) 6
West Virginia State University 7
Application Server configuration 7
WV Digital Identity Technology Hub **7**
Voter List Maintenance **8**
Ballot Verification Wizard **8**
4.1.1 Goals and Objectives **10**
Training 11
Support 11
Ballot Reuse 11
Mandatory Requirements **12**
4.1.2.1 12
4.1.2.2 12
4.1.2.4 12
4.1.2.5 12
4.1.2.6 13

SKYPUNCH
TECHNOLOGY

4.1.2.7 13
4.1.2.8 13
4.1.2.9 14
4.1.3.1.1 14
4.1.3.1.2 14
4.1.3.1.3 14
4.1.3.1.4 15
4.1.3.1.5 15
4.2 Qualifications and Experience 15
Signature Page 18

Introduction

Founded in 2002, Skypunch Technology (previously ElectionsOnline) is an original creator of online voting technology having supported thousands of elections ranging from small community groups to large professional associations including:

- American Statistical Association
  30,000+ voters
- Tennessee Consolidated Retirement System
  50,000+ voters
- District of Columbia Bar
  100,000+ voters

History

After relocating from Arlington, VA to Charleston, WV in 2018, Skypunch was welcomed in to *Vantage Ventures* (the accelerator within West Virginia University's John Chambers School of Business and Economics) and engages regularly with the university by providing experiential learning opportunities for students making meaningful contributions to Skypunch Technology as talked about later.

Cryptographic Ballot Verification

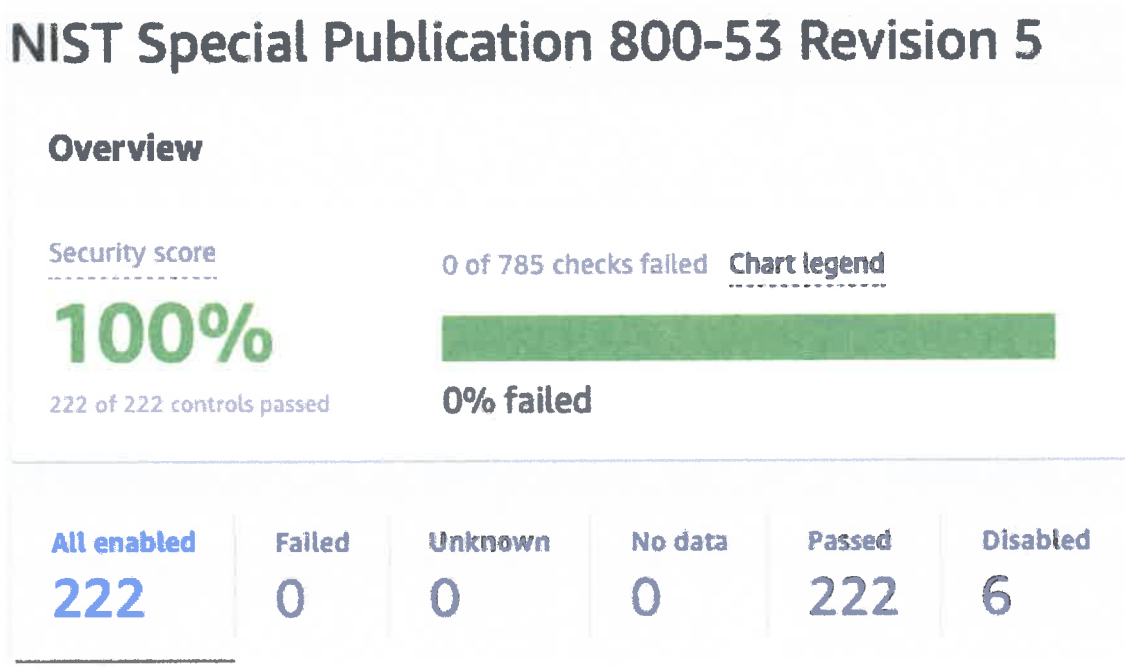
Skypunch is the only election service provider to have developed an ability for an individual voter to perform a *cryptographic* verification of their own ballot at any time after having cast that ballot. Never before have voters been so empowered to ensure their own ballot is not only accepted into the system, but absolutely not undergone any alteration whatsoever and is being counted. At a moment in our nation's history that is seeing a decline in voter confidence in our election apparatus, the Skypunch ballot verification wizard could not have arrived at a better time.

Cybersecurity

Special attention is warranted regarding the cybersecurity measures in place with the Skypunch system including the company's founder serving on the advisory board of the newly-launched *Cybersecurity Innovation Center* on the campus of West Virginia State University. Other noteworthy measures include:

National Institute of Standards and Technology (NIST) Special Publication 800-53

NIST SP 800-53 is the set of technology controls around which both FedRAMP and StateRAMP compliance is based. The Skypunch system is hosted in Amazon Web Services (AWS) and uses *Security Hub* (a tool within AWS) to assess the system's compliance with the technical controls in NIST SP 800-53. As seen in the following image pulled from the Security Hub welcome screen of Skypunch's AWS account, the system is 100% compliant with those controls. Also included with this proposal as a supporting document is a report showing the exact services audited and the NIST controls satisfied by them.



StateRAMP

Skypunch Technology is a member of StateRAMP and pursuing StateRAMP certification. The most challenging part of achieving that is compliance with the technical controls detailed in NIST SP 800-53 which, as stated above, is already accomplished.

Amazon Inspector

In addition to scanning the Skypunch system architecture with Security Hub, source code is also scanned by Amazon Inspector to ensure vulnerabilities in source code and package dependencies are patched in a timely manner once discovered.

Amazon Web Services (AWS) Certifications

AWS is known for being an especially secure platform but simply running a solution in the AWS cloud does not make it inherently secure. It takes expertise and the Skypunch voting solution is developed by architects and developers certified as:

Cybersecurity and Infrastructure Security Agency (CISA)

CISA uses industry-standard tools such as Nessus, Qualys, Burp Suite and Bugcrowd to scan the Skypunch Technology system and provide a weekly cyber hygiene report and monthly web application scan. The supporting documents include reports but the following image shows a cyber hygiene report card.

2023-09-08

CYBER HYGIENE

REPORT CARD

Skypunch Technology

CISA
CYBER+INFRASTRUCTURE

0 Hosts with unsupported software

0 Potentially Risky Open Services

100% Decrease in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

September 8, 2023 — September 8, 2023
Host Scans on All Addresses

September 8, 2023 — September 8, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
Decrease of 1
0% of hosts vulnerable

VULNERABILITIES

0
Decrease of 1

VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME

MAX AGE OF ACTIVE CRITICALS

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

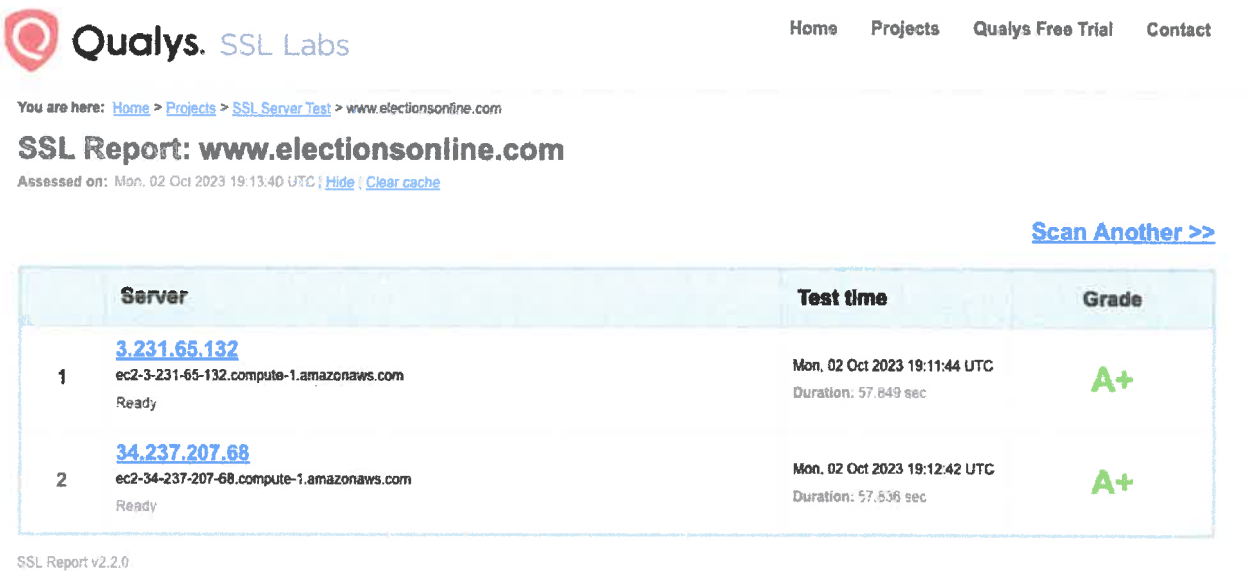
Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

**Denotes the possibility of a network management interface.*

SKYPUNCH
TECHNOLOGY

TLS configuration

The following screen image taken October 2, 2023 shows Skypunch earning an A+ for the TLS (transport layer security) configuration on its website.



Web Application Firewall (WAF) configuration

The following screen image (taken October 2, 2023) is included in response to the RFP's emphasis on OWASP vulnerabilities. The image demonstrates that a WAF is in place and has four rules sets enabled (enabled rules sets are shown with a blue slider just above the word "Edit"). A rule set is a collection of firewall rules that detect and deny potentially malicious requests. One of the enabled rule sets, the *Core rule set* focuses on, "vulnerabilities described in OWASP publications." The Supporting Documents includes a more fulsome report showing the exact rules enabled by each of the four rule sets.

Core rule set

Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. Learn More

700

Add to web ACL

Edit

Known bad inputs

Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. Learn More

200

Add to web ACL

Edit

Linux operating system

Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. Learn More

200

Add to web ACL

PHP application

Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. Learn More

100

Add to web ACL

POSIX operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not been allowed. Learn More

100

Add to web ACL

SQL database

Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Learn More

200

Add to web ACL

Edit

Windows operating system

Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code. Learn More

200

Add to web ACL

Edit

West Virginia University (WVU)

Using its residency in Vantage Ventures, Skypunch affords students at WVU with an experiential learning opportunity wherein they may carry out various cybersecurity related activities on the voting system. In the spring of 2023 this meant undergrads performing various vulnerability scanning activities on the system and in the summer of 2023 a five-person team of graduate

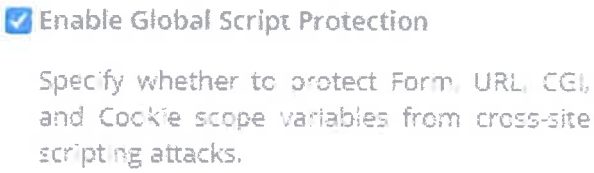
students assessed the system against the OWASP vulnerability checklist. Such activities are always under the supervision of university professors.

West Virginia State University

In 2024, the experiential learning opportunities taking place at WVU will expand to West Virginia State University, home of the newly-launched *Cybersecurity Innovation Center* where the Skypunch founder serves on the advisory board.

Application Server configuration

Inline with concerns found within OWASP controls pertaining to XSS attacks, the following screen image of the application server's administration console demonstrates the application server has enabled global script protection.



WV Digital Identity Technology Hub

Skypunch Technology was invited to submit a letter of support for West Virginia to be awarded more than one billion dollars of federal funding made available through the *CHIPS and Science Act* to develop a Digital Identity Technology Hub in West Virginia. Given that participating in an election demands proof of identity, and doing so online demands digital proof of identity, Skypunch is positioned to be squarely at the epicenter of some very exciting innovation as the world becomes more digitized. Senator Manchin's office announced on October 23 that West Virginia was indeed awarded this grant money.

Voter List Maintenance

Maintaining up-to-date voter records is a challenge for any jurisdiction. By adopting the Skypunch solution wherein voters are set up and recognized as *cloud voters*, it becomes possible to recognize when a West Virginia cloud voter moves to another state and is set up as a cloud voter there. In such a case, the WV Secretary of State could be notified that someone on their voter list is now apparently living elsewhere and should be removed from the WV list. Obviously such a benefit depends on the multi-state adoption of the Skypunch solution, but this could solve a downside of the United States not maintaining a national voter database.

Ballot Verification Wizard

Far surpassing simply allowing a voter to enter a ballot ID into some online service to confirm their ballot has been received, the Skypunch ballot verification wizard permits voters to effectively play an audit role by *cryptographically* verifying their ballot is captured; proven to have not been altered; and is being included in the tabulation. When a voter casts a ballot they receive an email confirmation moments later. That email contains: ballot id, digest, and tip address, plus a link to the online ballot verification wizard. At any time, the voter may visit that wizard; enter the data; and cryptographically verify their ballot. Explained in greater detail at www.electionsonline.com/verify/ballot-verification.cfm, the following screen image shows the moment in this wizard where a ballot is cryptographically proven to be unaltered. The voter also has the option to move on and see with their own eyes the selections made on the ballot.

Step 4 of 5—Get a proof and verify ballot

Provided digest hash

jZ3c3R6zjQcgbv6SDMZ6wS5040QwnJly+igoitA49IA=

Recalculated digest hash

jZ3c3R6zjQcgbv6SDMZ6wS5040QwnJly+igoitA49IA=

Verification status

Verified. 3bZ9nYh0FH01bevJqKeuAR is proven to have not been altered in any way since the time this digest was saved.

This ballot is proven to exist and be unaltered in the system of record, but should also be confirmed to exist in the reporting platform where election result tabulation is performed.

Proceed to confirm ballot is counted

4.1.1 Goals and Objectives

This project aims to provide a means by which to submit a ballot electronically for West Virginia residents serving overseas in the military along with disabled residents who may have difficulty accessing a polling station on election day. We call voters who choose to take advantage of this option *cloud voters*. Through multiple conversations with personnel in the WV SOS's office and others in the election administration business, the high level steps for accommodating that are:

1. Either the state or county communicates to such voters that being flagged as a cloud voter is a possibility.
2. Voters who wish to become cloud voters contact their county voter registration office and request to be flagged as a cloud voter in an upcoming election. From here, the process flows as diagrammed in attachment, Cloud Voter Registration in the Trade Secrets document.
3. Voting begins and cloud voters are informed by one of two methods of how to proceed to vote.
    a. Dynamic OTP (defined in Cloud Voter Registration) cloud voters are notified by email of how to proceed to the ballot and vote.
    b. Static OTP (defined in Cloud Voter Registration) cloud voters receive a paper notice including their one-time password for accessing the ballot. (Most voters, and particularly those overseas will be Dynamic OTP voters. Only residents without a smartphone on which to install an authenticator app are candidates for Static OTP voters.)
4. The voter accesses their ballot using two authentication factors: 1. a ballot access link they request at the moment they are ready to vote and which contains an access token that expires 10 minutes after being issued and 2. a time-based, one-time-password for

Dynamic OTP voters (defined above) or a one-time-password mailed to them by their jurisdiction if a Static OTP voter.

5. Upon casting their ballot, the voter receives an email confirmation that their ballot has been received. This email also contains the information needed by the voter to cryptographically verify their ballot should they so choose.
6. Voting concludes and the election administrator logs into their account on the Skypunch website to do two things:
    a. Perform verification. Verification is a two-step process that ensures all ballots are on version 0 as they should be and that there is one, and only one, match in the reporting system for each ballot that is in the system of record.
    b. Print out the ballot report. The ballot report shows the selections made on each and every ballot. It is understood that these selections will need to be re-entered by election administrators into a centralized tabulating system.

Training

Skypunch Technology will coordinate with SOS and county officials to develop a training timeline so that county election administrators who will need to create and thoroughly test the ballots described in the above are able to do so.

Support

Skypunch Technology uses *Teamwork* as its support ticketing system at no additional charge.

Ballot Reuse

Complex ballot setup can be time-consuming the first time. However, the Skypunch system permits a previous ballot configuration to be reused. This means that once election managers have gone through the process once, subsequent ballot setup goes extremely fast.

Mandatory Requirements

4.1.2.1

Over the past year, multiple conversations with personnel in the WV Secretary of State's office as well as outside parties involved with election administration reveal there is no uniformly accepted definition of what a "ballot design" file is. To some, use of the term "design" suggests it relates to font and color selection, to others it refers to the names of the candidates on the ballot. Regardless, the ballot setup and configuration process is as follows. Election managers (for example, at the county level) will have access to an account on the Skypunch website. Those managers may log in to that account and step through the election setup wizard–a very mature and user-friendly tool for entering those things to be voted on. Those managers will be provided training by Skypunch for how to create and configure ballots beginning in very early 2024.

4.1.2.2

The system is hosted in AWS and built around an immutable ledger database that permits cryptographic verification of each ballot by the voter as described earlier under the heading *Ballot Verification Wizard*. Within each client account an election manager may retrieve a *ballot report*. The report is nothing more but a printout of the voter selections made on each ballot to facilitate entry of those selections into a centralized tabulation system for in-county tallying.

4.1.2.4

With more than 20 years of providing election services, the Skypunch solution is one of the most mature available and benefits from years of usability expertise being applied to the ballot interface for as voter-friendly an experience as possible.

4.1.2.5

The solution permits this. It is not designed to be used in this manner given that a person who wishes to submit a paper ballot to the county clerk would not logically go through the cloud

voter setup process, but there is nothing stopping a person from making selections on an online ballot and then printing it out to mail in.

4.1.2.6

This is described earlier under the heading *Ballot Verification Wizard.* It is worth stating again here that the Skypunch solution to this matter far exceeds the requirement by permitting voters to perform a *cryptographic* verification of their ballot for absolute certainty it has not undergone any alteration–an enormously timely innovation.

4.1.2.7

Skypunch provides training and support throughout the entire duration of the contract. Most training will be conducted in online meetings, but there is the possibility for some in-person training as well.

4.1.2.8

To 4.1.2.8.1, the voting system is the ICT.

To 4.1.2.8.2, The ballot pages used by voters (though not the election management pages) of the system were audited for WCAG Level AA compliance by BeAccessible in mid-2022. Failed findings were uncovered but have been remediated. See the accompanying supporting document, *Accessibility Conformance Report.*

To 4.1.2.8.3, 4, 5 and 6, the system was audited by BeAccessible in mid-2022 using NVDA with Chrome as the primary screen reader. The website was also manually tested for conformance including and not limited to testing for keyboard-only users, heading levels, color contrast, and system timeout. The scope of that audit was limited to those pages used by voters plus the key parts of the ballot verification wizard which is incorporated into the main website. The scope did not include all other pages of that main website, nor the election management pages used by election managers to administer elections. Going through the audit was a learning experience

and anytime something new is developed and incorporated into the system, or something that exists already is modified, the lessons learned during the audit are incorporated into that new development. Going forward, it is anticipated that recurring audits by outside experts will happen on some set schedule so that typical user scenarios and tasks are kept current with the latest standards.

4.1.2.9

This requirement appears to be rolled into 4.1.3.1.3 and will be picked up there.

4.1.3.1.1

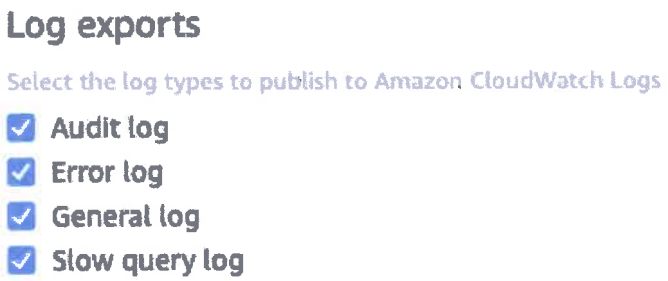
See attachment B plus the POA&M tracker.

4.1.3.1.2

The website is designed using responsive design principles making it suitable for both desktop and mobile viewing and negating the need for a separate mobile application.

4.1.3.1.3

See attachment D. Because attachment D deals heavily with database logging the following screen image of the database cluster's configuration settings demonstrates that all logging options are enabled for the cluster in question.



Attention should also be called to the previously-shared screen image showing 100% compliance with NIST controls given that many of those controls concern database configuration and security. It's also worth noting that Skypunch takes advantage of Amazon Web Services

Relational Database Service (RDS) which means the best database administrators in the world are in charge of configuring, optimizing and supporting the databases.

4.1.3.1.4

See attachment E.

4.1.3.1.5

See attachment F.

4.2 Qualifications and Experience

Skypunch Technology has been reliably providing web-based voting solutions since 2002, far longer than other similar companies have existed, making it one of the world's original creators of such. As stated in the opening, the service has been used in elections with as few as only a few dozen voters to those with more than 100,000 eligible voters spread globally. Please refer to the *Introduction* earlier in this proposal for more.

Personnel

David Simms–a member of the advisory board for the Cybersecurity Innovation Center at West Virginia State University–founded Skypunch Technology (previously ElectionsOnline, Inc.) in 2002. At the time he was the website developer for the District of Columbia Bar which needed to elect its Board of Directors and wanted to move away from paper and the postal service to do so. With nothing in the market, he was tasked with creating a solution which would be the harbinger of what has evolved into the solution offered today by Skypunch. He is also certified by Human Factors International as a Usability Analyst and has conducted usability studies for multiple sites to create measurable improvements to their user-friendliness and applied his experience as a technical writer to both create system documentation and provide the monthly Tech Notes column in the D.C. Bar's monthly publication, The Washington Lawyer. Additionally, he was managed or otherwise worked on several large-scale IT projects including such things as:

- Multiple website designs and redesigns
- Paper-to-electronic process re-engineering
- Deployment of expense accounting solutions
- CRM integrations
- Migrations to multiple Association Management Systems
- Intranet development

David's certifications include the following:

Andrea Gallagher has spent 25 years in software design and customer research in startups, consulting, Intuit, Google, and Asana. She is passionate about the needs of specialized experts with high-pressure critical roles. Relevant experience includes:

- For Intuit's white-labeled online banking service for regional banks and credit unions, lead the strategy project to understand the financial service managers and customer support representatives who used our admin tools to provide for their customers. Provided the team with a deep understanding of their users, the context, the goals, and the challenges. The admin tools team used this foundational roadmap to improve the user satisfaction rating immediately in the next release and continually over the next 3 years of development.

- Consulting work for a variety of clients building systems for complex processes and niche industries. We designed everything from corporate intranets to manufacturing supply chain marketplaces to commercial building maintenance hubs.
- For Invitrogen (now part of ThermoFischer Scientific), restructured the product data and searching tools that allowed life science laboratory managers to identify and source the products they needed for research and development.
- User insight for developer platforms at Intuit Quickbooks, Google Assistant, and Asana.

For this project, she will drive the customer success process, ensuring that all county clerks have the knowledge and tools they need to conduct online elections easily and efficiently.

Accessibility

BeAccessible, a leading company for conducting audits of systems intended for use by the disabled, has audited the Skypunch solution. There were findings which have since been remediated and Skypunch was provided the attached statement of accessibility by BeAccessible.

Exceeding Requirements

Skypunch is the first and only to have introduced to the world the ability for a voter to perform a *cryptographic* verification of their ballot. Enormously different from anything voters have heretofore been provided, this is presented earlier under the heading *Ballot Verification Wizard* and is the single biggest differentiator of the Skypunch solution. Please review the Introduction section of this proposal for more as there are a number of other differentiators presented there and it should also be added that while it was not listed in the requirements, Skypunch has enabled DNSSEC which is not a small thing to defend against DNS pollution.

Signature Page

REQUEST FOR PROPOSAL
West Virginia Secretary of State
RFP SOS2400000001
Election Division E-Ballot Delivery Technology

Example:
Proposal 1 Cost is $1,000,000
Proposal 2 Cost is $1,100,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

6.8. **Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Skypunch Technology
(Company)

David Giuliano President
(Representative Name, Title)

703-475-6504
(Contact Phone/Fax Number)

October 27, 2023
(Date)

Revised 01/01/2021

SKYPUNCH
TECHNOLOGY

WVSOS Election Division E-ballot Delivery Technology

Attachments and Addendums

CRFP 1600 SOS2400000001

Skypunch Technology
3803 Staunton Ave SE
Charleston WV 25304

Contact: David Simms
david@skypunch.tech
703-475-6504

www.skypunch.tech

Attachment B

OWASP Application Level Security Verification Levels 1-3

See supporting documentation from CISA, AWS Security Hub (NIST), the Web Application Firewall rule set. Also realize that both West Virginia University and West Virginia State University are regularly performing assessments of the system against OWASP controls as part of their experiential learning projects.

Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 1	Points for Meeting Requirements		Notes
Password Security Requirements			
Verify that user set passwords are at least 8 characters in length (after multiple spaces are combined).	5	N/A	Passwords are system-generated.
Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters.	5	N/A	See above.
Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space.	5	N/A	See above.
Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.	5	N/A	See above.
Verify users can change their password.	5	✓	
Verify that password change functionality requires the user's current and new password.	5	✓	It's worth nothing that changing a password is no different than resetting a forgotten password which does not require account login. The system follows the OWASP recommendations for password resets.
Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password.	5	N/A	Passwords are system-generated.
Verify that a password strength meter is provided to help users set a stronger password.	5	N/A	See above.
Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters.	5	N/A	See above.
Verify that there are no periodic credential rotation or password history requirements.	5	N/A	See above.

Verify that "paste" functionality, browser password helpers, and external password managers are permitted.	5	N/A	See above.
Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as built-in functionality.	5	✓	
General Authenticator Requirements			
Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.	5	✓	Verified to the extent the system utilizes reCAPTCHA at web-facing logins though does not limit failed attempts to 100 per hour per account.
Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.	5	✓	
Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.	5		See POA&M tracker.
Authenticator Lifecycle Requirements			
Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.	5	N/A	
Credential Recovery Requirements			

Verify that a system generated initial activation or recovery secret is not sent in clear text to the user.	5	✓	
Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.	5	✓	
Verify password credential recovery does not reveal the current password in any way.	5	✓	
Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").	5	✓	
Verify that if an authentication factor is changed or replaced, that the user is notified of this event.	5		See POA&M tracker.
Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as time-based OTP (TOTP) or other soft token, mobile push, or another offline recovery mechanism. (C6)	5	✓	
Out of Band Verifier Requirements			
Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.	5	✓	
Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.	5	✓	
Verify that the out of band verifier authentication requests, codes, or tokens are only usable once, and only for the original authentication request.	5	✓	
Verify that the out of band authenticator and verifier communicates over a secure independent channel.	5	✓	
Single or Multi-factor One Time Verifier Requirements			
Verify that time-based OTPs have a defined lifetime before expiring.	5	✓	
Fundamental Session Management Requirements			
Verify the application never reveals session tokens in URL parameters	5	✓	Verified with a caveat. The application never reveals it for browsers with cookies enabled. In the event a user's browser does not support cookies, the session token falls back to being passed in the URL.
Session Binding Requirements			

Verify the application generates a new session token on user authentication.	5	✓	
Verify that session tokens possess at least 64 bits of entropy.	5	✓	UUID's have 122 bits of entropy.
Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.	5	✓	
Session Logout and Timeout Requirements			
Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties.	5	✓	
Cookie-Based Session Management	5	✓	
Verify that cookie-based session tokens have the 'Secure' attribute set.	5	✓	
Verify that cookie-based session tokens have the 'HttpOnly' attribute set.	5	✓	
Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks.	5	✓	
Verify that cookie-based session tokens use "__Host-" prefix (see references) to provide session cookie confidentiality.	5		ColdFusion manages state with CFID and CFTOKEN which do not use the HOST prefix.
Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible.	5	✓	
General Access Control Design			
Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.	5	✓	
Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.	5	✓	
Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.	5	✓	

Verify that the principle of deny by default exists whereby new users/ roles start with minimal or no permissions and users/roles do not receive access to new features until access is explicitly assigned.	5	✓	
Verify that access controls fail securely including when an exception occurs.	5	✓	
Operation Level Access Control			
Verify that sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	5	✓	
Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.	5		See POA&M tracker.
Other Access Control Considerations			
Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.	5	✓	
Verify that directory browsing is disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of file or directory metadata, such as Thumbs.db, .DS_Store, .git or .svn folders.	5	✓	
Input Validation Requirements			
Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	5	✓	
Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.	5	✓	
Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists).	5	✓	
Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).	5	✓	

Verify that URL redirects and forwards only allow destinations which appear on an allow list, or show a warning when redirecting to potentially untrusted content.	5	✓	
Sanitization and Sandboxing Requirements			
Verify that all untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature.	5	✓	
Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.	5	✓	
Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.	5	✓	
Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.	5	✓	
Verify that the application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.	5	N/A	
Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, and uses allow lists of protocols, domains, paths and ports.	5	✓	
Verify that the application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.	5	N/A	
Verify that the application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.	5	✓	
Output Encoding and Injection Prevention Requirements			
Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ねこ or O'Hara).	5	✓	
Verify that output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled.	5	✓	

Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.	5	✓	
Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.	5	✓	
Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.	5	N/A	
Verify that the application protects against JavaScript or JSON injection attacks, including for eval attacks, remote JavaScript includes, Content Security Policy (CSP) bypasses, DOM XSS, and JavaScript expression evaluation.	5	N/A	
Verify that the application protects against LDAP injection vulnerabilities, or that specific security controls to prevent LDAP injection have been implemented.	5	N/A	
Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.	5	N/A	
Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.	5	N/A	
Verify that the application protects against XPath injection or XML injection attacks.	5	N/A	
Deserialization Prevention Requirements			
Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering.	5	✓	
Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks.	5	N/A	
Verify that deserialization of untrusted data is avoided or is protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).	5	✓	

Verify that when parsing JSON in browsers or JavaScript-based backends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.	5	✓	
Algorithms			
Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.	5	✓	
Log Content Requirements			
Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form.	5	✓	
Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy.	5	✓	
Error Handling			
Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate	5	✓	
Client-side Data Protection			
Verify the application sets sufficient anti-caching headers so that sensitive data is not cached in modern browsers.	5	✓	
Verify that data stored in browser storage (such as HTML5 local storage, session storage, IndexedDB, or cookies) does not contain sensitive data or PII.	5	✓	
Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated.	5	✓	
Sensitive Private Data			
Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.	5	✓	
Verify that users have a method to remove or export their data on demand.	5	✓	
Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.	5	✓	

Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data.	5	✓	
Deployed Application Integrity Controls			
Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.	5	N/A	
Verify that the application employs integrity protections, such as code signing or subresource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.	5	✓	
Verify that the application has protection from subdomain takeovers if the application relies upon DNS entries or DNS subdomains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (*autogen-bucket-id*.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.	5	✓	
Business Logic Security Requirements			
Verify the application will only process business logic flows for the same user in sequential step order and without skipping steps.	5	✓	
Verify the application will only process business logic flows with all steps being processed in realistic human time, i.e. transactions are not submitted too quickly.	5	✓	
Verify the application has appropriate limits for specific business actions or transactions which are correctly enforced on a per user basis.	5	✓	
Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.	5	✓	AWS Shield and GuardDuty are enabled.
Verify the application has business logic limits or validation to protect against likely business risks or threats, identified using threat modeling or similar methodologies.	5	✓	See above.
File Upload Requirements			

Verify that the application will not accept large files that could fill up storage or cause a denial of service.	5	✓	
File Execution Requirements			
Verify that user-submitted filename metadata is not used directly by system or framework filesystems and that a URL API is used to protect against path traversal.	5	✓	
Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure, creation, updating or removal of local files (LFI).	5	N/A	
Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure or execution of remote files via Remote File Inclusion (RFI) or Server-side Request Forgery (SSRF) attacks.	5	N/A	
Verify that the application protects against Reflective File Download (RFD) by validating or ignoring user-submitted filenames in a JSON, JSONP, or URL parameter, the response Content-Type header should be set to text/plain, and the Content-Disposition header should have a fixed filename.	5	N/A	
Verify that untrusted file metadata is not used directly with system API or libraries, to protect against OS command injection.	5	N/A	
File Storage Requirements			
Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions, preferably with strong validation.	5	✓	
Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload of known malicious content.	5		They are not scanned, but do go to an S3 bucket outside the VPC where they pose no harm.
File Download Requirements			
Verify that the web tier is configured to serve only files with specific file extensions to prevent unintentional information and source code leakage. For example, backup files (e.g. .bak), temporary working files (e.g. .swp), compressed files (.zip, .tar.gz, etc) and other extensions commonly used by editors should be blocked unless required.	5	✓	
Verify that direct requests to uploaded files will never be executed as HTML/JavaScript content.	5	✓	
SSRF Protection Requirements			

Verify that the web or application server is configured with an allow list of resources or systems to which the server can send requests or load data/files from.	5	✓	While there is no allow list configured on the server, there is discussion within OWASP as to whether this is a duplicate of control 5.2.6 regarding SSRF attacks which was verified, hence the checkbox.
Generic Web Service Security Verification Requirements			
Verify that all application components use the same encodings and parsers to avoid parsing attacks that exploit different URI or file parsing behavior that could be used in SSRF and RFI attacks.	5	✓	
Verify that access to administration and management functions is limited to authorized administrators.	5	✓	
Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.	5	✓	
RESTful Web Service Verification Requirements			
Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.	5	✓	
Verify that JSON schema validation is in place and verified before accepting input.	5	✓	
Verify that RESTful web services that utilize cookies are protected from Cross-Site Request Forgery via the use of at least one or more of the following: double submit cookie pattern, CSRF nonces, or Origin request header checks.	5	N/A	
SOAP Web Service Verification Requirements			
Verify that XSD schema validation takes place to ensure a properly formed XML document, followed by validation of each input field before any processing of that data takes place.	5	N/A	
Dependency			
Verify that all components are up to date, preferably using a dependency checker during build or compile time.	5	✓	

Verify that all unneeded features, documentation, samples, configurations are removed, such as sample applications, platform documentation, and default or example users.	5	✓	
Verify that if application assets, such as JavaScript libraries, CSS or web fonts, are hosted externally on a Content Delivery Network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.	5	✓	
Unintended Security Disclosure Requirements			
Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures.	5	✓	
Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.	5	✓	
Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.	5	✓	
HTTP Security Headers Requirements			
Verify that every HTTP response contains a Content-Type header. text/*, /+xml and application/xml content types should also specify a safe character set (e.g., UTF-8, ISO-8859-1).	5	✓	
Verify that all API responses contain a Content-Disposition: attachment; filename="api.json" header (or other appropriate filename for the content type).	5	N/A	
Verify that a Content Security Policy (CSP) response header is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.	5	✓	
Verify that all responses contain a X-Content-Type-Options: nosniff header.	5	✓	

Verify that a Strict-Transport-Security header is included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.	5	✓	
Verify that a suitable "Referrer-Policy" header is included, such as "no-referrer" or "same-origin".	5	✓	
Verify that the content of a web application cannot be embedded in a third-party site by default and that embedding of the exact resources is only allowed where necessary by using suitable Content-Security-Policy: frame-ancestors and X-Frame-Options response headers.	5	✓	
Validate HTTP Request Header Requirements			
Verify that the application server only accepts the HTTP methods in use by the application/API, including pre-flight OPTIONS, and logs/alerts on any requests that are not valid for the application context.	5	✓	
Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.	5	✓	
Verify that the Cross-Origin Resource Sharing (CORS) Access-Control-Allow-Origin header uses a strict allow list of trusted domains and subdomains to match against and does not support the "null" origin.	5	✓	
Select Controls from Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 2			
Secure Software Development Lifecycle			
Verify the use of a secure software development lifecycle that addresses security in all stages of development	3	✓	
Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.	3	✓	
Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls.	3	✓	

Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.	3	✓	
Authentication Architectural Requirements			
Verify that communications between application components, including APIs, middleware and data layers, are authenticated. Components should have the least necessary privileges needed	3	✓	
Verify that the application uses a single vetted authentication mechanism that is known to be secure, can be extended to include strong authentication, and has sufficient logging and monitoring to detect account abuse or breaches.	3	✓	
Verify that all authentication pathways and identity management APIs implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.	3	✓	
Access Control Architectural Requirements			
Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.	3	✓	
Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.	3	✓	
Verify that attribute or feature-based access control is used whereby the code checks the user's authorization for a feature/data item rather than just their role. Permissions should still be allocated using roles.	3	✓	
Input and Output Architectural Requirements			
Verify that input and output requirements clearly define how to handle and process data based on type, content, and applicable laws, regulations, and other policy compliance.	3	✓	

Verify that serialization is not used when communicating with untrusted clients. If this is not possible, ensure that adequate integrity controls (and possibly encryption if sensitive data is sent) are enforced to prevent deserialization attacks including object injection.	3	✓
Cryptographic Architectural Requirements		
Verify that there is an explicit policy for management of cryptographic keys and that a cryptographic key lifecycle follows a key management standard such as NIST SP 800-57.	3	✓
Verify that consumers of cryptographic services protect key material and other secrets by using key vaults or API based alternatives.	3	✓
Verify that all keys and passwords are replaceable and are part of a well-defined process to re-encrypt sensitive data.	3	✓
Verify that the architecture treats client-side secrets--such as symmetric keys, passwords, or API tokens--as insecure and never uses them to protect or access sensitive data.	3	✓
Errors, Logging and Auditing Architectural Requirements		
Verify that a common logging format and approach is used across the system.	3	✓
Verify that logs are securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation.	3	✓
Data Protection and Privacy Architectural Requirements		
Verify that all sensitive data is identified and classified into protection levels.	3	✓
Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.	3	✓
Communications Architectural Requirements		

Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers.	3	✓	Verified
Verify that application components verify the authenticity of each side in a communication link to prevent person-in-the-middle attacks. For example, application components should validate TLS certificates and chains.	3	✓	All data in transit and at rest (with the exception of load balancer to app server) is encrypted. Certificate validation however does not occur in every instance.
Malicious Software Architectural Requirements			
Verify that a source code control system is in use, with procedures to ensure that check-ins are accompanied by issues or change tickets. The source code control system should have access control and identifiable users to allow traceability of any changes.	3	✓	
Secure File Upload Architectural Requirements			
Verify that user-uploaded files are stored outside of the web root.	3	✓	
Verify that user-uploaded files - if required to be displayed or downloaded from the application - are served by either octet stream downloads, or from an unrelated domain, such as a cloud file storage bucket. Implement a suitable Content Security Policy (CSP) to reduce the risk from XSS vectors or other attacks from the uploaded file.	3	✓	
Configuration Architectural Requirements			
Verify the segregation of components of differing trust levels through well-defined security controls, firewall rules, API gateways, reverse proxies, cloud-based security groups, or similar mechanisms.	3	✓	
Verify that the build pipeline warns of out-of-date or insecure components and takes appropriate actions.	3	✓	
Verify that the build pipeline contains a build step to automatically build and verify the secure deployment of the application, particularly if the application infrastructure is software defined, such as cloud environment build scripts.	3	N/A	

Verify that application deployments adequately sandbox, containerize and/or isolate at the network level to delay and deter attackers from attacking other applications, especially when they are performing sensitive or dangerous actions such as deserialization.	3	✓	
Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.	3	✓	
Credential Storage Requirements			
Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash	3	✓	Argon2id is in use.
Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored.	3	✓	Verified, but with the default 16 bit salt length.
Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations.	3	N/A	
Credential Recovery Requirements			
Verify that if OTP or multi-factor authentication factors are lost, that evidence of identity proofing is performed at the same level as during enrollment.	3	✓	
Look-up Secret Verifier Requirements			
Verify that lookup secrets can be used only once.	3	N/A	
Verify that lookup secrets have sufficient randomness (112 bits of entropy), or if less than 112 bits of entropy, salted with a unique and random 32-bit salt and hashed with an approved one-way hash.	3	N/A	
Verify that lookup secrets are resistant to offline attacks, such as predictable values.	3	N/A	

Out of Band Verifier Requirements			
Verify that the out of band verifier retains only a hashed version of the authentication code.	3	N/A	
Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).	3	✓	
Single or Multi-factor One Time Verifier Requirements			
Verify that symmetric keys used to verify submitted OTPs are highly protected, such as by using a hardware security module or secure operating system based key storage.	3		Secrets are stored on an encrypted drive.
Verify that approved cryptographic algorithms are used in the generation, seeding, and verification of OTPs.	3	✓	
Verify that time-based OTP can be used only once within the validity period.	3		See POA&M tracker.
Verify that if a time-based multi-factor OTP token is re-used during the validity period, it is logged and rejected with secure notifications being sent to the holder of the device.	3		See POA&M tracker.
Cryptographic Software and Devices Verifier Requirements			
Verify that cryptographic keys used in verification are stored securely and protected against disclosure, such as using a Trusted Platform Module (TPM) or Hardware Security Module (HSM), or an OS service that can use this secure storage.	3	N/A	
Verify that the challenge nonce is at least 64 bits in length, and statistically unique or unique over the lifetime of the cryptographic device.	3	N/A	
Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.	3	N/A	
Service Authentication Requirements			

Verify that if passwords are required for service authentication, the service account used is not a default credential. (e.g. root/root or admin/ admin are default in some services during installation).	3	✓	
Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.	3	✓	
Session Binding Requirements			
Verify that session token are generated using approved cryptographic algorithms.	3	✓	https://helpx.adobe.com/coldfusion/cfml-reference/coldfusion-functions/functions-c-d/CreateUUID.html
Session Logout and Timeout Requirements			
Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.	3		See POA&M tracker.
Verify that users are able to view and (having re-entered login credentials) log out of any or all currently active sessions and devices.	3		See above.
Token-Based Session Management			
Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.	3	✓	
Verify that stateless session tokens use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.	3	N/A	
Other Access Control Considerations			
Verify the application has additional authorization (such as step up or adaptive authentication) for lower value systems, and / or segregation of duties for high value applications to enforce anti-fraud controls as per the risk of application and past fraud.	3	N/A	
Data Classificiation			

Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.	3	✓	
Algorithms			
Verify that industry proven or government approved cryptographic algorithms, modes, and libraries are used, instead of custom coded cryptography.	3	✓	Cryptography and encryption is very often built into the AWS services used by Skypunch and may therefore be trusted to employ the most modern and robust tools available for that.
Verify that encryption initialization vector, cipher configuration, and block modes are configured securely using the latest advice.	3	✓	See above.
Verify that random number, encryption or hashing algorithms, key lengths, rounds, ciphers or modes, can be reconfigured, upgraded, or swapped at any time, to protect against cryptographic breaks.	3	✓	See above.
Verify that known insecure block modes (i.e. ECB, etc.), padding modes (i.e. PKCS#1 v1.5, etc.), ciphers with small block sizes (i.e. Triple-DES, Blowfish, etc.), and weak hashing algorithms (i.e. MD5, SHA1, etc.) are not used unless required for backwards compatibility.	3	✓	See above.
Verify that nonces, initialization vectors, and other single use numbers must not be used more than once with a given encryption key. The method of generation must be appropriate for the algorithm being used.	3	✓	See above.
Random Values			
Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved cryptographically secure random number generator when these random values are intended to be not guessable by an attacker.	3	✓	https://helpx.adobe.com/coldfusion/cfml-reference/coldfusion-functions/functions-c-d/CreateUUID.html

Verify that random GUIDs are created using the GUID v4 algorithm, and a Cryptographically-secure Pseudo-random Number Generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.	3	✓	Difficult to verify but most likely. "The ColdFusion UUID generation algorithm uses the unique time-of-day value, the IEEE 802 Host ID, and a cryptographically strong random number generator to generate UUIDs that conform to the principles laid out in the draft IEEE RFC "*UUIDs and GUIDs*."
Secret Management			
Verify that a secrets management solution such as a key vault is used to securely create, store, control access to and destroy secrets.	3	✓	Parameter Store of Systems Manager
Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations	3	✓	
Log Content Requirements			
Verify that the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures.	3	✓	
Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens	3	✓	
Log Processing Requirements			
Verify that all authentication decisions are logged, without storing sensitive session tokens or passwords. This should include requests with relevant metadata needed for security investigations.	3	✓	
Verify that all access control decisions can be logged and all failed decisions are logged. This should include requests with relevant metadata needed for security investigations.	3	✓	
Log Protection Requirements			
Verify that the application appropriately encodes user-supplied data to prevent log injection.	3	✓	
Verify that all events are protected from injection when viewed in log viewing software.	3	✓	

Verify that security logs are protected from unauthorized access and modification.	3	✓	
Verify that time sources are synchronized to the correct time and time zone. Strongly consider logging only in UTC if systems are global to assist with post-incident forensic analysis.	3	✓	
Error Handling			
Verify that a "last resort" error handler is defined which will catch all unhandled exceptions.	3	✓	https://www.electionsonline.com/error.cfm
General Data Protection			
Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.	3	✓	
Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.	3	N/A	
Verify the application minimizes the number of parameters in a request, such as hidden fields, Ajax variables, cookies and header values.	3	N/A	
Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application.	3	✓	AWS GuardDuty detects abnormal activity.
Sensitive Private Data			
Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.	3	N/A	As defined by the EU and others for GDPR and the like, the system does not store sensitive private data on users.
Verify that sensitive information contained in memory is overwritten as soon as it is no longer required to mitigate memory dumping attacks, using zeroes or random data.	3	N/A	See above.
Verify that sensitive or private information that is required to be encrypted, is encrypted using approved algorithms that provide both confidentiality and integrity.	3	N/A	See above.

Verify that sensitive personal information is subject to data retention classification, such that old or out of date data is deleted automatically, on a schedule, or as the situation requires.	3	N/A	See above.
Client Communications Security Requirements			
Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols.	3	✓	TLS and SSH, when appropriate, are used.
Verify using online or up to date TLS testing tools that only strong algorithms, ciphers, and protocols are enabled, with the strongest algorithms and ciphers set as preferred.	3	✓	Screenshot from Qualys Labs in the Technical Proposal.
Verify that old versions of SSL and TLS protocols, algorithms, ciphers, and configuration are disabled, such as SSLv2, SSLv3, or TLS 1.0 and TLS 1.1. The latest version of TLS should be the preferred cipher suite.	3	✓	See above.
Server Communications Security Requirements			
Verify that connections to and from the server use trusted TLS certificates. Where internally generated or self-signed certificates are used, the server must be configured to only trust specific internal CAs and specific self-signed certificates. All others should be rejected.	3	✓	As tested at https://www.ssllabs.com/ssltest/
Verify that encrypted communications such as TLS is used for all inbound and outbound connections, including for management ports, monitoring, authentication, API, or web service calls, database, cloud, serverless, mainframe, external, and partner connections. The server must not fall back to insecure or unencrypted protocols.	3	✓	See above.
Verify that all encrypted connections to external systems that involve sensitive information or functions are authenticated.	3	✓	See above.
Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.	3	✓	See above.
Malicious Code Search			

Verify that the application source code and third party libraries do not contain unauthorized phone home or data collection capabilities. Where such functionality exists, obtain the user's permission for it to operate before collecting any data.	3	✓	
Verify that the application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.	3	✓	
Business Logic Security Requirements			
Verify the application has configurable alerting when automated attacks or unusual activity is detected.	3	✓	GuardDuty
File Integrity Requirements			
Verify that files obtained from untrusted sources are validated to be of expected type based on the file's content.	3	✓	
File Execution Requirements			
Verify that the application does not include and execute functionality from untrusted sources, such as unverified content distribution networks, JavaScript libraries, node npm libraries, or server-side DLLs.	3	✓	
RESTful Web Service Verification Requirements			
Verify that the message headers and payload are trustworthy and not modified in transit. Requiring strong encryption for transport (TLS only) may be sufficient in many cases as it provides both confidentiality and integrity protection. Per-message digital signatures can provide additional assurance on top of the transport protections for high-security applications but bring with them additional complexity and risks to weigh against the benefits.	3	✓	
SOAP Web Service Verification Requirements			
Verify that the message payload is signed using WS-Security to ensure reliable transport between client and service.	3	N/A	
GraphQL and other Web Service Data Layer Security Requirements			

Verify that a query allow list or a combination of depth limiting and amount limiting is used to prevent GraphQL or data layer expression Denial of Service (DoS) as a result of expensive, nested queries. For more advanced scenarios, query cost analysis should be used.	3	N/A	
Build			
Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.	3	✓	Verified partially. Deployments are not automated, but are secure and repeatable.
Verify that compiler flags are configured to enable all available buffer overflow protections and warnings, including stack randomization, data execution prevention, and to break the build if an unsafe pointer, memory, format string, integer, or string operations are found.	3	✓	The application is nearly immune to buffer overflow as it's written in Java (ColdFusion) and Python which are immune with the exception of overflows in their interpreters. (https://www.fortinet.com/resources/cyberglossary/buffer-overflow)
Verify that server configuration is hardened as per the recommendations of the application server and frameworks in use.	3	✓	
Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.	3	✓	
Dependency			
Verify that third party components come from pre-defined, trusted and continually maintained repositories	3	✓	pypl.org
Verify that the attack surface is reduced by sandboxing or encapsulating third party libraries to expose only the required behaviour into the application	3	✓	Lambda functions run inside containers, each with very narrowly defined purpose.
Validate HTTP Request Header Requirements			
Verify that HTTP headers added by a trusted proxy or SSO devices, such as a bearer token, are authenticated by the application.	3	N/A	

Select Controls from Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 3			
General Authenticator Requirements			
Verify impersonation resistance against phishing, such as the use of multi-factor authentication, cryptographic devices with intent (such as connected keys with a push to authenticate), or at higher AAL levels, client-side certificates.	1	✓	
Verify that where a Credential Service Provider (CSP) and the application verifying authentication are separated, mutually authenticated TLS is in place between the two endpoints.	1	N/A	
Session Logout and Timeout Requirements			
If authenticators permit users to remain logged in, verify that re-authentication occurs periodically with 2FA both when actively used after 12 hours or after an idle period of 15 minutes	1	✓	Re-authentication is necessary after 40 minutes in the administrative application, 20 minutes for the voter application.
Algorithms			
Verify that encrypted data is authenticated via signatures, authenticated cipher modes, or HMAC to ensure that ciphertext is not altered by an unauthorized party	1	✓	Skypunch offloads all encryption to AWS.
General Data Protection			
Verify that regular backups of important data are performed and that test restoration of data is performed.	1	✓	App and database servers are included in nightly backup plans.
Verify that backups are stored securely to prevent data from being stolen or corrupted.	1	✓	Backups are stored in the AWS cloud.
Code Integrity Controls			
Verify that a code analysis tool is in use that can detect potentially malicious code, such as time functions, unsafe file operations and network connections.	1	✓	Amazon Inspector.
Malicious Code Search			

Verify that the application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered.	1	✓	Verified with the caveat from the Amazon Inspector documentation, "At this time Amazon Inspector vulnerability database search only supports searching for CVE IDs, however, Amazon Inspector tracks, and produces findings for, other software vulnerabilities in the database."
Verify that the application source code and third party libraries do not contain time bombs by searching for date and time related functions.	1	✓	See above.
Verify that the application source code and third party libraries do not contain malicious code, such as salami attacks, logic bypasses, or logic bombs.	1	✓	See above.
Verify that the application source code and third party libraries do not contain Easter eggs or any other potentially unwanted functionality.	1	✓	See above.
Total Possible Points	**955**		

Attachment D

Security Requirements for Databases

Skypunch Technology relies on Amazon Web Services Relational Database Service. In addition to the listed requirements, it should be noted that the database cluster, like the application server, resides in a private subnet–not publicly accessible–of the Skypunch Virtual Private Cloud. Regarding its security configuration, the following should be observed:

- FIPS 140-2 services
  https://aws.amazon.com/compliance/fips/
  Being that this is a public document, the exact database in use will not be listed in this document, but it is listed on the FIPS page from AWS.
- Compliance
  https://aws.amazon.com/compliance/ (general compliance information)
- RDBMS compliance
  https://aws.amazon.com/compliance/services-in-scope/FedRAMP/
  Again, being that this will be a public document, the exact services in use by Skypunch will not be listed in this document, but are found on the Services in Scope page for FedRAMP.
- DoD compliance
  https://aws.amazon.com/compliance/services-in-scope/DoD_CC_SRG/
  The RDBMS in use by Skypunch is found listed on the Services in Scope for DoD also.

Select Controls from Department of Defense - Security Requirements Guide for Databases (Moderate Controls)	Points for Meeting Requirements		
The DBMS must limit the number of concurrent sessions to an organization-defined number per user for all accounts and/or account types.	3	✓	
The DBMS must protect against a user falsely repudiating having performed organization-defined actions.	MANDATORY	✓	
The DBMS must be able to generate audit records when privileges/permissions are retrieved.	3	✓	
The DBMS must be able to generate audit records when unsuccessful attempts to retrieve privileges/permissions occur.	3	✓	
The DBMS must initiate session auditing upon startup.	MANDATORY	✓	
The DBMS must produce audit records containing sufficient information to establish what type of events occurred.	3	✓	
The DBMS must produce audit records containing time stamps to establish when the events occurred.	3	✓	
The DBMS must produce audit records containing sufficient information to establish where the events occurred.	MANDATORY	✓	
The DBMS must produce audit records containing sufficient information to establish the sources (origins) of the events.	MANDATORY	✓	
The DBMS must produce audit records containing sufficient information to establish the outcome (success or failure) of the events.	3	✓	
The DBMS must produce audit records containing sufficient information to establish the identity of any user/subject or process associated with the event.	3	✓	
The DBMS must include additional, more detailed, organization-defined information in the audit records for audit events identified by type, location, or subject.	3	✓	

The DBMS must by default shut down upon audit failure, to include the unavailability of space for more audit log records; or must be configurable to shut down upon audit failure.	3	N/A	An audit failure due to an unavailability of space is not applicable considering the audit logs are sent to CloudWatch and the database storage capacity grows dynamically when needed. This database cluster also is configured for high availability meaning that if an instance within the cluster fails, another replica comes online instantly. This enormously desirable behavior makes a shut down on audit failure not applicable.
The DBMS must be configurable to overwrite audit log records, oldest first (First-In-First-Out - FIFO), in the event of unavailability of space for more audit log records.	MANDATORY	N/A	See above.
The DBMS must use system clocks to generate time stamps for use in audit records and application data.	3	✓	
The audit information produced by the DBMS must be protected from unauthorized read access.	MANDATORY	✓	
The audit information produced by the DBMS must be protected from unauthorized modification.	MANDATORY	✓	
The audit information produced by the DBMS must be protected from unauthorized deletion.	MANDATORY	✓	
The DBMS must protect its audit features from unauthorized access.	MANDATORY	✓	
The DBMS must protect its audit configuration from unauthorized modification.	MANDATORY	✓	
The DBMS must protect its audit features from unauthorized removal.	MANDATORY	✓	
The DBMS must limit privileges to change software modules, to include stored procedures, functions and triggers, and links to software external to the DBMS.	3	✓	
The DBMS software installation account must be restricted to authorized users.	MANDATORY	✓	

Database software, including DBMS configuration files, must be stored in dedicated directories, or DASD pools, separate from the host OS and other applications.	3	✓	A customer of AWS RDS would not have visibility into such things but as provided at https://aws.amazon.com/compliance/, "Inherit the most comprehensive compliance controls with AWS. AWS supports 143 security standards and compliance certifications, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy compliance requirements around the globe."
Database objects (including but not limited to tables, indexes, storage, stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be owned by database/DBMS principals authorized for ownership.	3	✓	
The role(s)/group(s) used to modify database structure (including but not necessarily limited to tables, indexes, storage, etc.) and logic modules (stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be restricted to authorized users.	MANDATORY	✓	
Default demonstration and sample databases, database objects, and applications must be removed.	3	✓	
Unused database components, DBMS software, and database objects must be removed.	3	✓	
Unused database components that are integrated in the DBMS and cannot be uninstalled must be disabled.	3	✓	
Access to external executables must be disabled or restricted.	3	✓	
The DBMS must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	3	✓	
If passwords are used for authentication, the DBMS must store only hashed, salted representations of passwords.	MANDATORY	✓	
If passwords are used for authentication, the DBMS must transmit only encrypted representations of passwords.	MANDATORY	✓	

The DBMS must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	3	✓	
The DBMS must use NIST FIPS 140-2 validated cryptographic modules for cryptographic operations.	MANDATORY	✓	https://aws.amazon.com/compliance/fips/
The DBMS must separate user functionality (including user interface services) from database management functionality.	3	✓	
The DBMS must invalidate session identifiers upon user logout or other session termination.	MANDATORY	✓	The databases in use by Skypunch are DoD and FedRAMP compliant. Without referencing exact technologies, given that this will be a public document, one may visit both https://aws.amazon.com/compliance/services-in-scope/FedRAMP/ (for FedRAMP compliant services) and https://aws.amazon.com/compliance/services-in-scope/DoD_CC_SRG/ (for DoD compliant services) and see the database services used by Skypunch among those listed. When combined with the screen image shared in the main proposal document showing 100% compliance with NIST 800-53 controls for the Skypunch architecture and services configuration, one may be assured the solution meets the most demanding security requirements including this one given that compliance with those standards requires this behavior.
The DBMS must recognize only system-generated session identifiers.	3	✓	See above.
The DBMS must maintain the authenticity of communications sessions by guarding against man-in-the-middle attacks that guess at Session ID values.	MANDATORY	✓	See above.
The DBMS must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	3	✓	

In the event of a system failure, the DBMS must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	MANDATORY	✓	
The DBMS must protect the confidentiality and integrity of all information at rest.	MANDATORY	✓	
The DBMS must isolate security functions from non-security functions.	MANDATORY	✓	
Total Points	**66**		

Attachment E

Select Controls from the StateRAMP Moderate Baseline

StateRAMP, like FedRAMP, is driven by NIST SP 800-53. Among the supporting documents, pay special attention to the report from AWS Security Hub showing 100% compliance with the NIST controls applicable to the Skypunch environment.

Select Controls from the StateRAMP Moderate Baseline	Points for Meeting Requirements		
Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	MANDATORY	✓	
Limit system access to the types of transactions and functions that authorized users are permitted to execute.	MANDATORY	✓	
Monitor and control remote access sessions.	MANDATORY	✓	
Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	MANDATORY	✓	
Authorize wireless access prior to allowing such connections.	5	✓	
Protect wireless access using authentication and encryption.	MANDATORY	✓	
Control connection of mobile devices.	5	✓	
Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	MANDATORY	✓	
Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	MANDATORY	✓	
Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	MANDATORY	✓	
Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	MANDATORY	✓	
Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	5	✓	
Establish and enforce security configuration settings for information technology products employed in organizational systems.	MANDATORY	✓	
Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5	✓	
Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	MANDATORY	✓	

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	MANDATORY	✓	
Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	MANDATORY	✓	
Identify system users, processes acting on behalf of users, and devices.	MANDATORY	✓	
Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5	✓	
Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	MANDATORY	✓	
Store and transmit only cryptographically-protected passwords.	MANDATORY	✓	
Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	MANDATORY	✓	
Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	MANDATORY	✓	
Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5	✓	
Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5	✓	
Control the use of removable media on system components.	MANDATORY	✓	
Ensure that organizational systems containing sensitive data are protected during and after personnel actions such as terminations and transfers.	MANDATORY	✓	
Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	MANDATORY	✓	
Protect and monitor the physical facility and support infrastructure for organizational systems.	5	✓	
Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	MANDATORY	✓	

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	5	✓	
Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	5	✓	
Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	MANDATORY	✓	
Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	MANDATORY	✓	
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	MANDATORY	✓	
Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	MANDATORY	✓	
Protect the authenticity of communications sessions.	5	✓	
Identify, report, and correct system flaws in a timely manner.	MANDATORY	✓	
Provide protection from malicious code at designated locations within organizational systems.	MANDATORY	✓	
Monitor system security alerts and advisories and take action in response.	MANDATORY	✓	
Update malicious code protection mechanisms when new releases are available.	MANDATORY	✓	
Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	MANDATORY	✓	
Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	✓	
Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3	✓	
Perform maintenance on organizational systems.	3	✓	
Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3	✓	
Prohibit the use of portable storage devices when such devices have no identifiable owner.	3	✓	

Screen individuals prior to authorizing access to organizational systems containing sensitive data	3	✓	
Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of sensitive data.	3	✓	
Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3	✓	
Implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive data during transmission unless otherwise protected by alternative physical safeguards.	3	✓	
Employ FIPS-validated cryptography when used to protect the confidentiality of sensitive data.	3	✓	
Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3	✓	
Identify unauthorized use of organizational systems	3	✓	
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	✓	
Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	✓	
Limit unsuccessful logon attempts.	1		See POA&M tracker
Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	1	✓	
Terminate (automatically) a user session after a defined condition.	1	✓	
Route remote access via managed access control points.	1	✓	
Verify and control/limit connections to and use of external systems.	1	✓	
Limit use of portable storage devices on external systems.	1	✓	
Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1	✓	

Review and update logged events.	1	✓	
Alert in the event of an audit logging process failure.	1	✓	
Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1	✓	
Limit management of audit logging functionality to a subset of privileged users.	1	✓	
Analyze the security impact of changes prior to implementation.	1	✓	
Control and monitor user-installed software.	1	✓	
Enforce a minimum password complexity and change of characters when new passwords are created.	1	✓	
Allow temporary password use for system logons with an immediate change to a permanent password.	1	✓	
Obscure feedback of authentication information.	1	✓	
Test the organizational incident response capability.	1	✓	
Supervise the maintenance activities of maintenance personnel without required access authorization.	1	✓	
Protect the confidentiality of backup sensitive data at storage locations.	1	✓	
Escort visitors and monitor visitor activity.	1	✓	
Remediate vulnerabilities in accordance with risk assessments.	1	✓	
Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	1	✓	
Establish and manage cryptographic keys for cryptography employed in organizational systems.	1	✓	
Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	MANDATORY	✓	
Total Possible Points	**116**		

Attachment F

Plan of Action & Milestones Tracker

System Name:

POA&M ID	Type	Scheduled Completion Date	Mitigating Factors	Comments
Attachement B, line 18.	General Authenticator Requirements	November 13, 2023	Send a profile change email to user(s) of affected accounts.	
Attachement B, line 26	Credential Recovery Requirements	November 13, 2023	To be completed with the line above.	
Attachement B, line 57	Operation Level Access Control	November 20, 2023	https://helpx.adobe.com/coldfusion/cfml-reference/coldfusion-functions/functions-c-d/CSRFGenerateToken.html	A strong CSRF token is already generated and available for use across the entire site. However, it is not being used as often as it could be. That can and will be used in every occasion possible across the entirely of the site by the scheduled completion date.
Attachement B, line 222 and 223.	Single or multi-factor one time verifier requirements	12/11/2023	Development work required to enable this.	
Attachement B, line 234	Session Logout and Timeout Requirements	1/11/2024	Development work required to enable this.	
Auto insurance	Insurance	Post award.	The purchase of $1,000,000 automobile liability coverage.	There is an offer from the insurance company, good until the end of November 2023, to provide the $1,000,000 automobile liability coverage. Pending award of the contract, that policy may go into effect.
Cyber insurance	Insurance	Post award.	Increase cyber insurance from $1,000,000 to $3,000,000.	This offer has already been put in place with the insurance company and is ready to go into effect pending award of the contract.

Addendums

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SOS24*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Skypunch Technology
Company

David Simons
Authorized Signature

September 27, 2023
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SOS24*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[ ]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Skypunch Technology
Company

David Simms
Authorized Signature

October 28, 2023
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

WVSOS Election Division E-ballot Delivery Technology

Supporting Documents

CRFP 1600 SOS2400000001

Skypunch Technology
3803 Staunton Ave SE
Charleston WV 25304

Contact: David Simms
david@skypunch.tech
703-475-6504

www.skypunch.tech

Supporting Document

NIST Special Publication 800-53 Revision 5 audit

The following report is from the October 13, 2023 nightly audit of the entire system architecture as performed by Security Hub–a service within Amazon Web Services–against the controls defined in NIST Special Publication 800-53 Revision 5.

Compliance Status	Severity	ID	Title	Failed checks	Passed checks	Related requirements
Passed	Critical	CloudFront.1	CloudFront distributions should have a default root object configured	0	2	NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16)
Passed	Critical	CodeBuild.1	CodeBuild GitHub or Bitbucket source repository URLs should use OAuth	0	1	NIST.800-53.r5 SA-3
Passed	Critical	CodeBuild.2	CodeBuild project environment variables should not contain clear text credentials	0	1	NIST.800-53.r5 IA-5(7), NIST.800-53.r5 SA-3
Passed	Critical	DMS.1	Database Migration Service replication instances should not be public	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	EC2.1	EBS snapshots should not be publicly restorable	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	EC2.19	Security groups should not allow unrestricted access to ports with high risk	0	9	NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)
Passed	Critical	ES.2	Elasticsearch domains should be in a VPC	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	IAM.4	IAM root user access key should not exist	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2)
Passed	Critical	IAM.6	Hardware MFA should be enabled for the root user	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-2(1), NIST.800-53.r5 IA-2(2), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-2(8)
Passed	Critical	IAM.9	MFA should be enabled for the root user	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-2(1), NIST.800-53.r5 IA-2(2), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-2(8)
Passed	Critical	KMS.3	AWS KMS keys should not be deleted unintentionally	0	2	NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12(2)
Passed	Critical	Lambda.1	Lambda function policies should prohibit public access	0	37	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	Neptune.3	Neptune DB cluster snapshots should not be public	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	Opensearch.2	OpenSearch domains should be in a VPC	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	RDS.1	RDS snapshot should be private	0	10	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	RDS.2	RDS DB Instances should prohibit public access, as determined by the PubliclyAccessible configuration	0	2	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	Redshift.1	Amazon Redshift clusters should prohibit public access	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	S3.2	S3 buckets should prohibit public read access	0	12	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	S3.3	S3 buckets should prohibit public write access	0	12	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Critical	SSM.4	SSM documents should not be public	0	7	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	Account.2	AWS account should be part of an AWS Organizations organization	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

Passed	High	AutoScaling.3	Auto Scaling group launch configurations should configure EC2 instances to require Instance Metadata Service Version 2 (IMDSv2)	0	1	NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	High	AutoScaling.4	Auto Scaling group launch configuration should not have a metadata response hop limit greater than 1	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	High	Autoscaling.5	Amazon EC2 instances launched using Auto Scaling group launch configurations should not have Public IP addresses	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	CloudFront.12	CloudFront distributions should not point to non-existent S3 origins	0	2	NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	High	CloudTrail.1	CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events	0	1	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8(22)
Passed	High	CloudWatch.15	CloudWatch Alarms should have an action configured for the alarm state	0	1	NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4(1), NIST.800-53.r5 IR-4(5), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)
Passed	High	CloudWatch.17	CloudWatch alarm actions should be enabled	0	1	NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4(12)
Passed	High	CodeBuild.5	CodeBuild project environments should not have privileged mode enabled	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2)
Passed	High	EC2.13	Security groups should not allow ingress from 0.0.0.0/0 to port 22	0	9	NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)
Passed	High	EC2.18	Security groups should only allow unrestricted incoming traffic for authorized ports	0	2	NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)
Passed	High	EC2.2	VPC default security groups should not allow inbound or outbound traffic	0	1	NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)
Passed	High	EC2.23	EC2 Transit Gateways should not automatically accept VPC attachment requests	0	1	NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	High	EC2.25	EC2 launch templates should not assign public IPs to network interfaces	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	EC2.8	EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	0	3	NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6
Passed	High	EC2.9	EC2 instances should not have a public IPv4 address	0	2	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	ECR.1	ECR private repositories should have image scanning configured	0	1	NIST.800-53.r5 RA-5
Passed	High	ECS 0.10	Amazon ECS task definitions should have secure networking modes and user definitions.	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6
Passed	High	ECS 0.20	ECS services should not have public IP addresses assigned to them automatically	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	ECS 0.30	ECS task definitions should not share the host's process namespace	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	High	ECS 0.40	ECS containers should run as non-privileged	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6
Passed	High	ECS 0.50	ECS containers should be limited to read-only access to root filesystems	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6
Passed	High	ECS 0.60	Secrets should not be passed as container environment variables	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	High	EKS.1	EKS cluster endpoints should not be publicly accessible	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	EKS.2	EKS clusters should run on a supported Kubernetes version	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)
Passed	High	EMR.1	Amazon Elastic MapReduce cluster master nodes should not have public IP addresses	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	ElasticBeanstalk.2	Elastic Beanstalk managed platform updates should be enabled	0	1	NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

Passed	High	GuardDuty.1	GuardDuty should be enabled	0	1	NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3(4), NIST.800-53.r5 SA-11(1), NIST.800-53.r5 SA-11(6), NIST.800-53.r5 SA-15(2), NIST.800-53.r5 SA-15(8), NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SA-8(21), NIST.800-53.r5 SA-8(25), NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5(1), NIST.800-53.r5 SC-5(3), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4(13), NIST.800-53.r5 SI-4(2), NIST.800-53.r5 SI-4(22), NIST.800-53.r5 SI-4(25), NIST.800-53.r5 SI-4(4), NIST.800-53.r5 SI-4(5)
Passed	High	IAM.1	IAM policies should not allow full "*" administrative privileges"	0	27	NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2), NIST.800-53.r5 AC-6(3)
Passed	High	Opensearch.7	OpenSearch domains should have fine-grained access control enabled	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6
Passed	High	RDS.13	RDS automatic minor version upgrades should be enabled	0	2	NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)
Passed	High	RDS.16	RDS instances should be deployed in a VPC	0	2	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	S3.6	S3 permissions granted to other AWS accounts in bucket policies should be restricted	0	12	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	High	S3.8	S3 Block Public Access setting should be enabled at the bucket-level	0	12	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	SSM.2	EC2 instances managed by Systems Manager should have a patch compliance status of COMPLIANT after a patch installation	0	1	NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(3), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)
Passed	High	SageMaker.1	Amazon SageMaker notebook instances should not have direct internet access	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	SageMaker.2	SageMaker notebook instances should be launched in a custom VPC	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	High	SageMaker.3	Users should not have root access to SageMaker notebook instances	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2)
Passed	Medium	ACM.1	Imported and ACM-issued certificates should be renewed after a specified time period	0	4	NIST.800-53.r5 SC-28(3), NIST.800-53.r5 SC-7(16)
Passed	Medium	APIGateway.1	API Gateway REST and WebSocket API execution logging should be enabled	0	1	NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)
Passed	Medium	APIGateway.2	API Gateway REST API stages should be configured to use SSL certificates for backend authentication	0	1	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	APIGateway.4	API Gateway should be associated with a WAF Web ACL	0	1	NIST.800-53.r5 AC-4(21)
Passed	Medium	APIGateway.5	API Gateway REST API cache data should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	APIGateway.8	API Gateway routes should specify an authorization type	0	4	NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Medium	APIGateway.9	Access logging should be configured for API Gateway V2 Stages	0	1	NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)
Passed	Medium	Account.1	Security contact information should be provided for an AWS account.	0	1	NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Medium	Athena.1	Athena workgroups should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	AutoScaling.2	Amazon EC2 Auto Scaling group should cover multiple Availability Zones	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	AutoScaling.6	Auto Scaling groups should use multiple instance types in multiple Availability Zones	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	AutoScaling.9	EC2 Auto Scaling groups should use EC2 launch templates	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

Passed	Medium	CloudFront.10	CloudFront distributions should not use deprecated SSL protocols between edge locations and custom origins	0	1	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	CloudFront.3	CloudFront distributions should require encryption in transit	0	2	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	CloudFront.5	CloudFront distributions should have logging enabled	0	2	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	CloudFront.6	CloudFront distributions should have WAF enabled	0	2	NIST.800-53.r5 AC-4(21)
Passed	Medium	CloudFront.7	CloudFront distributions should use custom SSL/TLS certificates	0	2	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	CloudFront.9	CloudFront distributions should encrypt traffic to custom origins	0	1	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	CloudTrail.2	CloudTrail should have encryption at-rest enabled	0	1	NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	CloudWatch.16	CloudWatch log groups should be retained for at least 1 year	0	52	NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12
Passed	Medium	CodeBuild.4	CodeBuild project environments should have a logging configuration	0	1	NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	Config.1	AWS Config should be enabled	0	1	NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6(1), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(2)
Passed	Medium	DocumentDB.1	Amazon DocumentDB clusters should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	DocumentDB.2	Amazon DocumentDB clusters should have an adequate backup retention period	0	1	NIST.800-53.r5 SI-12
Passed	Medium	DynamoDB.1	DynamoDB tables should automatically scale capacity with demand	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	DynamoDB.2	DynamoDB tables should have point-in-time recovery enabled	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)
Passed	Medium	DynamoDB.3	DynamoDB Accelerator (DAX) clusters should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	DynamoDB.4	DynamoDB tables should be present in a backup plan	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)
Passed	Medium	EC2.15	EC2 subnets should not automatically assign public IP addresses	0	10	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Medium	EC2.20	Both VPN tunnels for an AWS Site-to-Site VPN connection should be up	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	EC2.21	Network ACLs should not allow ingress from 0.0.0.0/0 to port 22 or port 3389	0	1	NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(5)
Passed	Medium	EC2.24	EC2 paravirtual instance types should not be used	0	3	NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Medium	EC2.3	Attached EBS volumes should be encrypted at-rest	0	3	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	EC2.4	Stopped EC2 instances should be removed after a specified time period	0	2	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Medium	EC2.6	VPC flow logging should be enabled in all VPCs	0	1	NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7(8)
Passed	Medium	EC2.7	EBS default encryption should be enabled	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Passed	Medium	ES.8	Connections to Elasticsearch domains should be encrypted using TLS 1.2	0	1	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	IAM.19	MFA should be enabled for all IAM users	0	2	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-2(1), NIST.800-53.r5 IA-2(2), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-2(8)
Passed	Medium	IAM.3	IAM users' access keys should be rotated every 90 days or less	0	2	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-2(3), NIST.800-53.r5 AC-3(15)
Passed	Medium	IAM.5	MFA should be enabled for all IAM users that have a console password	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-2(1), NIST.800-53.r5 IA-2(2), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-2(8)
Passed	Medium	IAM.7	Password policies for IAM users should have strong configurations	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-2(3), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-5(1)
Passed	Medium	IAM.8	Unused IAM user credentials should be removed	0	2	NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-2(3), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6
Passed	Medium	KMS.1	IAM customer managed policies should not allow decryption actions on all KMS keys	0	27	NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(3)
Passed	Medium	KMS.2	IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys	0	59	NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(3)
Passed	Medium	KMS.4	AWS KMS key rotation should be enabled	0	1	NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12(2), NIST.800-53.r5 SC-28(3)
Passed	Medium	Kinesis.1	Kinesis streams should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	Lambda.2	Lambda functions should use supported runtimes	0	37	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(3)
Passed	Medium	Lambda.5	VPC Lambda functions should operate in more than one Availability Zone	0	37	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	Neptune.1	Neptune DB clusters should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	Neptune.2	Neptune DB clusters should publish audit logs to CloudWatch Logs	0	1	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-4(5), NIST.800-53.r5 SI-7(8)
Passed	Medium	Neptune.5	Neptune DB clusters should have automated backups enabled	0	1	NIST.800-53.r5 SI-12
Passed	Medium	Neptune.6	Neptune DB cluster snapshots should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(6)
Passed	Medium	Neptune.7	Neptune DB clusters should have IAM database authentication enabled	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6
Passed	Medium	NetworkFirewall.3	Network Firewall policies should have at least one rule group associated	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	NetworkFirewall.4	The default stateless action for Network Firewall policies should be drop or forward for full packets	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	NetworkFirewall.5	The default stateless action for Network Firewall policies should be drop or forward for fragmented packets	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	NetworkFirewall.6	Stateless network firewall rule group should not be empty	0	1	NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(5)
Passed	Medium	Opensearch.1	OpenSearch domains should have encryption at rest enabled	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)
Passed	Medium	Opensearch.3	OpenSearch domains should encrypt data sent between nodes	0	1	NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)
Passed	Medium	Opensearch.4	OpenSearch domain error logging to CloudWatch Logs should be enabled	0	1	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	Opensearch.5	OpenSearch domains should have audit logging enabled	0	1	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	Opensearch.6	OpenSearch domains should have at least three data nodes	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Passed	Medium	Opensearch.8	Connections to OpenSearch domains should be encrypted using TLS 1.2	0	1	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	RDS.10	IAM authentication should be configured for RDS instances	0	2	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6
Passed	Medium	RDS.11	RDS instances should have automatic backups enabled	0	2	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)
Passed	Medium	RDS.12	IAM authentication should be configured for RDS clusters	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6
Passed	Medium	RDS.15	RDS DB clusters should be configured for multiple Availability Zones	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	RDS.24	RDS Database Clusters should use a custom administrator username	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	RDS.25	RDS database instances should use a custom administrator username	0	2	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	RDS.26	RDS DB instances should be protected by a backup plan	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)
Passed	Medium	RDS.27	RDS DB clusters should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	RDS.3	RDS DB instances should have encryption at-rest enabled	0	2	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	RDS.4	RDS cluster snapshots and database snapshots should be encrypted at rest	0	10	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	RDS.5	RDS DB instances should be configured with multiple Availability Zones	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	RDS.9	Database logging should be enabled	0	2	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	Redshift.10	Redshift clusters should be encrypted at rest	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)
Passed	Medium	Redshift.2	Connections to Amazon Redshift clusters should be encrypted in transit	0	1	NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)
Passed	Medium	Redshift.3	Amazon Redshift clusters should have automatic snapshots enabled	0	1	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-13(5)
Passed	Medium	Redshift.4	Amazon Redshift clusters should have audit logging enabled	0	1	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	Redshift.6	Amazon Redshift should have automatic upgrades to major versions enabled	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)
Passed	Medium	Redshift.7	Redshift clusters should use enhanced VPC routing	0	1	NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Medium	Redshift.8	Amazon Redshift clusters should not use the default Admin username	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	Redshift.9	Redshift clusters should not use the default database name	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	S3.1	S3 Block Public Access setting should be enabled	0	1	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Medium	S3.10	S3 buckets with versioning enabled should have lifecycle policies configured	0	12	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Medium	S3.11	S3 buckets should have event notifications enabled	0	12	NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(4)
Passed	Medium	S3.12	S3 access control lists (ACLs) should not be used to manage user access to buckets	0	12	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6
Passed	Medium	S3.15	S3 buckets should be configured to use Object Lock	0	12	NIST.800-53.r5 CP-6(2)

Passed	Medium	S3.5	S3 buckets should require requests to use Secure Socket Layer	0	12	NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)
Passed	Medium	S3.9	S3 bucket server access logging should be enabled	0	10	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)
Passed	Medium	SNS.1	SNS topics should be encrypted at-rest using AWS KMS	0	4	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	SQS.1	Amazon SQS queues should be encrypted at rest	0	4	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)
Passed	Medium	SSM.1	EC2 instances should be managed by AWS Systems Manager	0	3	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-15(2), NIST.800-53.r5 SA-15(6), NIST.800-53.r5 SA-3, NIST.800-53.r5 SI-2(3)
Passed	Medium	SecretsManager.1	Secrets Manager secrets should have automatic rotation enabled	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)
Passed	Medium	SecretsManager.2	Secrets Manager secrets configured with automatic rotation should rotate successfully	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)
Passed	Medium	SecretsManager.3	Remove unused Secrets Manager secrets	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)
Passed	Medium	SecretsManager.4	Secrets Manager secrets should be rotated within a specified number of days	0	1	NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)
Passed	Medium	WAF.1	AWS WAF Classic Global Web ACL logging should be enabled	0	1	NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)
Passed	Medium	WAF.10	AWS WAF web ACLs should have at least one rule or rule group	0	3	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	WAF.2	AWS WAF Classic Regional rules should have at least one condition	0	1	NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21)
Passed	Medium	WAF.3	AWS WAF Classic Regional rule groups should have at least one rule	0	1	NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21)
Passed	Medium	WAF.4	AWS WAF Classic Regional web ACLs should have at least one rule or rule group	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	WAF.6	AWS WAF Classic global rules should have at least one condition	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	WAF.7	AWS WAF Classic global rule groups should have at least one rule	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Medium	WAF.8	AWS WAF Classic global web ACLs should have at least one rule or rule group	0	1	NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21)
Passed	Low	APIGateway.3	API Gateway REST API stages should have AWS X-Ray tracing enabled	0	1	NIST.800-53.r5 CA-7
Passed	Low	AutoScaling.1	Auto scaling groups associated with a Classic Load Balancer should use load balancer health checks	0	1	NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 SI-2
Passed	Low	CloudFormation.1	CloudFormation stacks should be integrated with Simple Notification Service (SNS)	0	2	NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)
Passed	Low	CloudFront.4	CloudFront distributions should have origin failover configured	0	2	NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Low	CloudFront.8	CloudFront distributions should use SNI to serve HTTPS requests	0	2	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2
Passed	Low	CloudTrail.4	CloudTrail log file validation should be enabled	0	1	NIST.800-53.r5 AU-9, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7(1), NIST.800-53.r5 SI-7(3), NIST.800-53.r5 SI-7(7)
Passed	Low	CloudTrail.5	CloudTrail trails should be integrated with Amazon CloudWatch Logs	0	1	NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-4(5), NIST.800-53.r5 SI-7(8)
Passed	Low	CodeBuild.3	CodeBuild S3 logs should be encrypted	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)
Passed	Low	EC2.12	Unused EC2 EIPs should be removed	0	2	NIST.800-53.r5 CM-8(1)
Passed	Low	EC2.16	Unused Network Access Control Lists should be removed	0	1	NIST.800-53.r5 CM-8(1)
Passed	Low	EC2.17	EC2 instances should not use multiple ENIs	0	3	NIST.800-53.r5 AC-4(21)
Passed	Low	EC2.28	EBS volumes should be in a backup plan	0	2	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)
Passed	Low	ElasticBeanstalk.1	Elastic Beanstalk environments should have enhanced health reporting enabled	0	1	NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2
Passed	Low	IAM.2	IAM users should not have IAM policies attached	0	2	NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(3)

Passed	Low	IAM.21	IAM customer managed policies that you create should not allow wildcard actions for services	0	27	NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2), NIST.800-53.r5 AC-6(3)
Passed	Low	Lambda.3	Lambda functions should be in a VPC	0	37	NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)
Passed	Low	Neptune.4	Neptune DB clusters should have deletion protection enabled	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)
Passed	Low	Neptune.8	Neptune DB clusters should be configured to copy tags to snapshots	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Low	RDS.16	RDS DB clusters should be configured to copy tags to snapshots	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Low	RDS.17	RDS DB instances should be configured to copy tags to snapshots	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)
Passed	Low	RDS.19	Existing RDS event notification subscriptions should be configured for critical cluster events	0	1	NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2
Passed	Low	RDS.20	Existing RDS event notification subscriptions should be configured for critical database instance events	0	1	NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2
Passed	Low	RDS.21	An RDS event notifications subscription should be configured for critical database parameter group events	0	1	NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2
Passed	Low	RDS.22	An RDS event notifications subscription should be configured for critical database security group events	0	1	NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2
Passed	Low	RDS.23	RDS instances should not use a database engine default port	0	2	NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)
Passed	Low	RDS.7	RDS clusters should have deletion protection enabled	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 SC-5(2)
Passed	Low	RDS.8	RDS DB instances should have deletion protection enabled	0	1	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)
Passed	Low	S3.13	S3 buckets should have lifecycle policies configured	0	12	NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)
Passed	Low	S3.14	S3 buckets should have versioning enabled	0	12	NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)
Passed	Low	SSM.3	EC2 instances managed by Systems Manager should have an association compliance status of COMPLIANT	0	3	NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SI-2(3)
Passed	Low	WAF.11	AWS WAF web ACL logging should be enabled	0	3	NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Supporting Document

Cyber Hygiene Reports

The following collection of reports--provided by CISA--are performed weekly and use industry-standard tools to look for vulnerabilities in internet-facing systems that may have weak configurations and/or known vulnerabilities.

2023-10-10

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

October 10, 2023 — October 10, 2023
Host Scans on All Addresses

No vulnerability scans yet
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

0
No Change

SERVICES

0
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

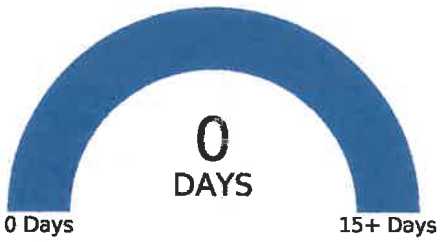
VULNERABILITIES

0
No Change

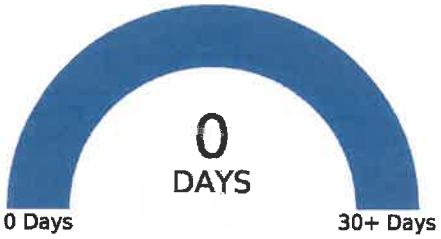
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-10-03

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

100% Decrease in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

October 3, 2023 — October 3, 2023
Host Scans on All Addresses

No vulnerability scans yet
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

0
Decrease of 1

SERVICES

0
Decrease of 1

VULNERABLE HOSTS

0
Decrease of 1
0% of hosts vulnerable

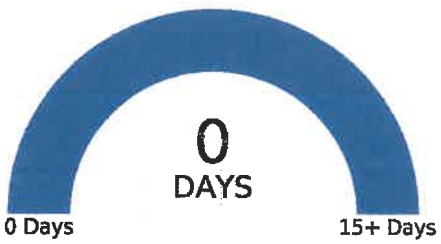
VULNERABILITIES

0
Decrease of 2

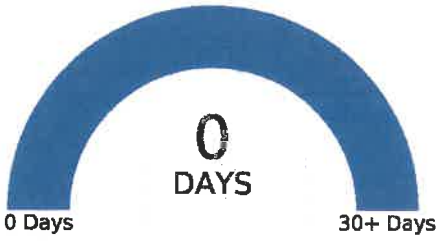
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-09-27

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

September 27, 2023 — September 27, 2023
Host Scans on All Addresses

September 27, 2023 — September 27, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

1
Decrease of 1

VULNERABLE HOSTS

1
Increase of 1
100% of hosts vulnerable

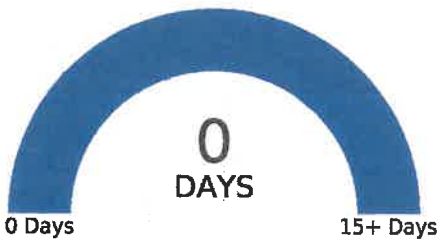
VULNERABILITIES

2
Increase of 2

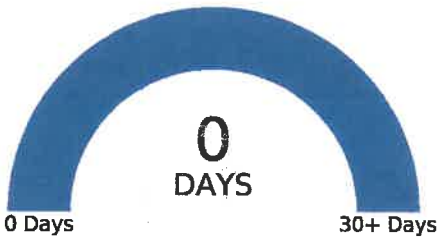
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-09-20

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

September 20, 2023 — September 20, 2023
Host Scans on All Addresses

September 20, 2023 — September 20, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

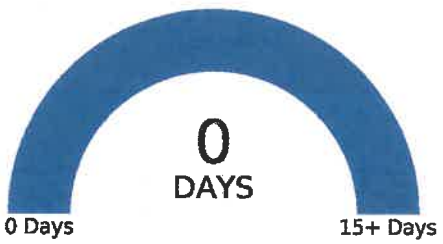
VULNERABILITIES

0
No Change

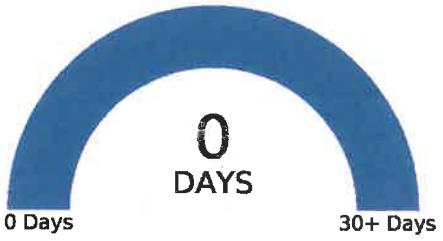
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-09-13

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

September 13, 2023 — September 14, 2023
Host Scans on All Addresses

September 14, 2023 — September 14, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

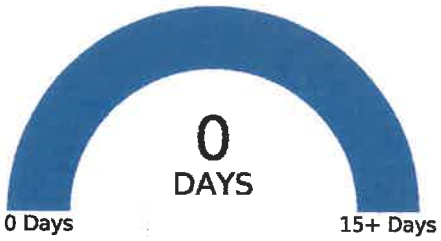
VULNERABILITIES

0
No Change

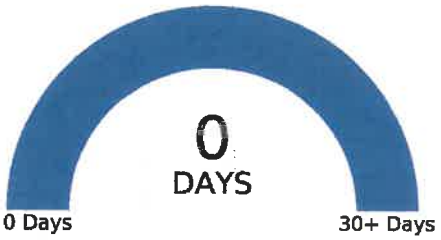
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open Open, No New Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-09-08

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

100% Decrease in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

September 8, 2023 — September 8, 2023
Host Scans on All Addresses

September 8, 2023 — September 8, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
Decrease of 1
0% of hosts vulnerable

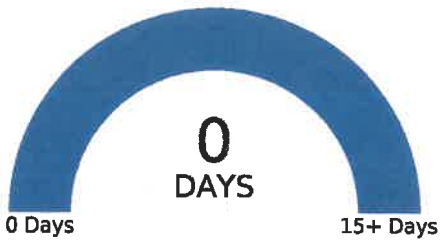
VULNERABILITIES

0
Decrease of 1

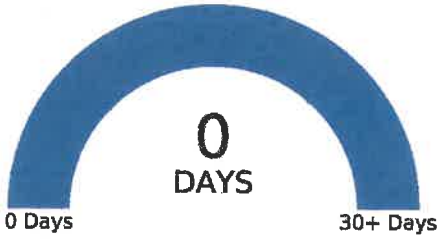
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-08-31

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

August 31, 2023 — August 31, 2023
Host Scans on All Addresses

August 31, 2023 — August 31, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

1
Increase of 1
100% of hosts vulnerable

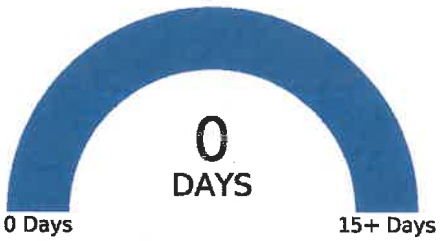
VULNERABILITIES

1
Increase of 1

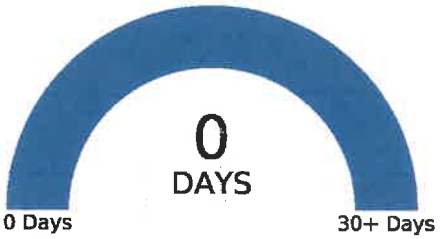
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-08-24

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

August 24, 2023 — August 24, 2023
Host Scans on All Addresses

August 24, 2023 — August 24, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

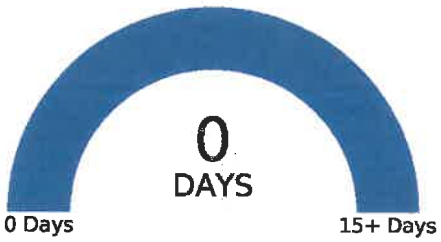
VULNERABILITIES

0
No Change

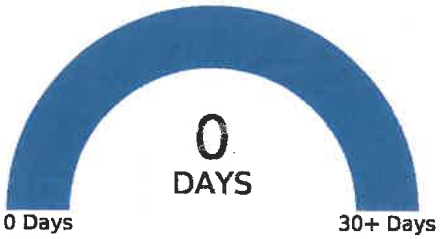
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-08-17

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

August 17, 2023 — August 17, 2023
Host Scans on All Addresses

August 17, 2023 — August 17, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

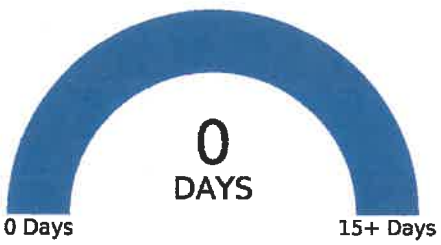
VULNERABILITIES

0
No Change

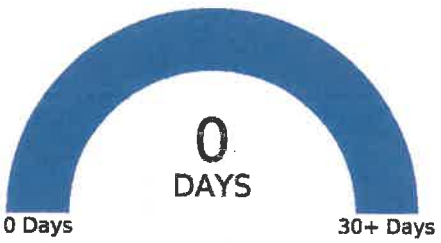
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-08-10

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

August 10, 2023 — August 10, 2023
Host Scans on All Addresses

August 10, 2023 — August 10, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

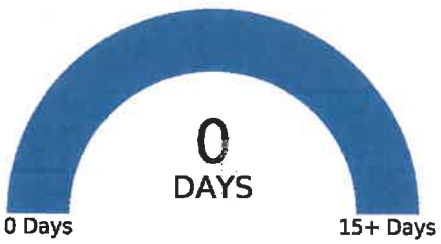
VULNERABILITIES

0
No Change

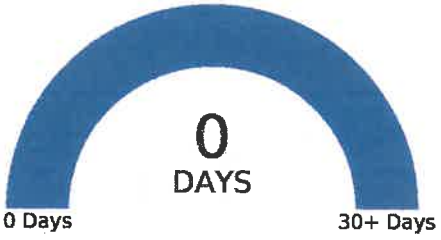
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-08-03

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

August 3, 2023 — August 3, 2023
Host Scans on All Addresses

August 3, 2023 — August 3, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

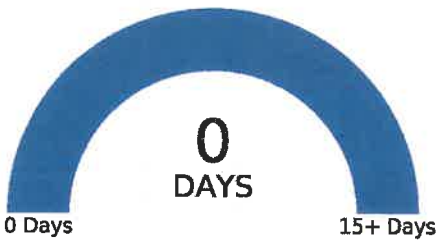
VULNERABILITIES

0
No Change

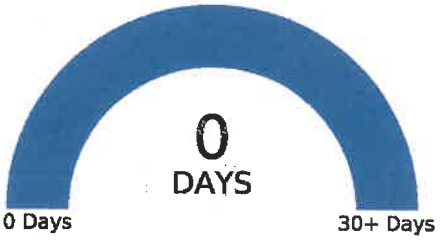
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP* 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

2023-07-27

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

July 27, 2023 — July 27, 2023
Host Scans on All Addresses

July 27, 2023 — July 27, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

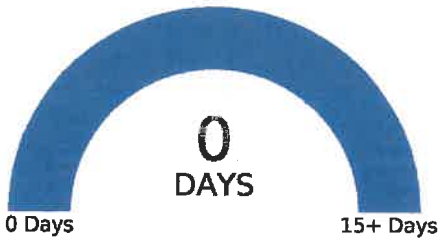
VULNERABILITIES

0
No Change

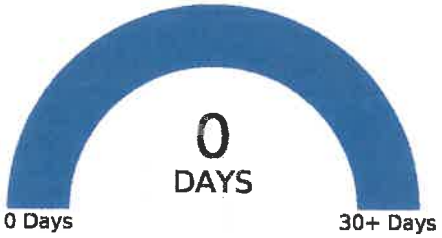
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open Open, No New Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

2023-07-20

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

July 20, 2023 — July 20, 2023
Host Scans on All Addresses

July 20, 2023 — July 20, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

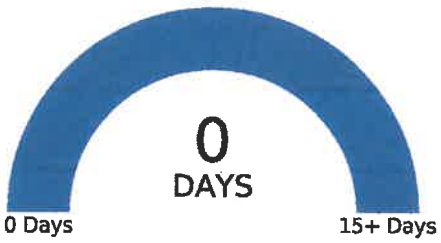
VULNERABILITIES

0
No Change

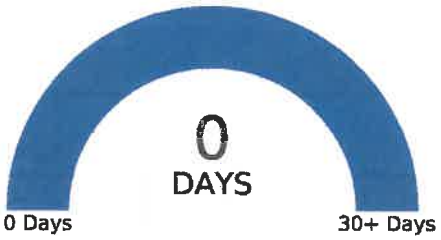
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open Open, No New Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

2023-07-14

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

July 14, 2023 — July 14, 2023
Host Scans on All Addresses

July 14, 2023 — July 14, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

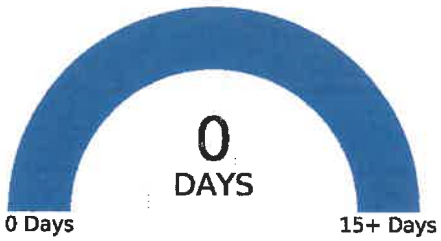
VULNERABILITIES

0
No Change

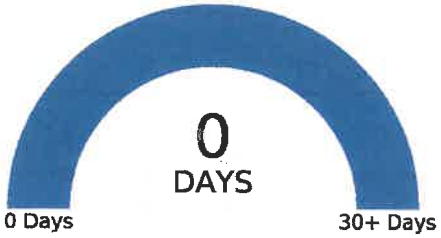
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open Open, No New Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

2023-07-09

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

100%
Decrease in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

July 9, 2023 — July 9, 2023
Host Scans on All Addresses

July 9, 2023 — July 9, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
Decrease of 1
0% of hosts vulnerable

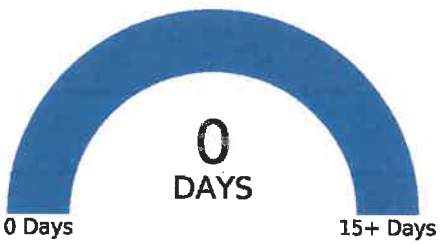
VULNERABILITIES

0
Decrease of 1

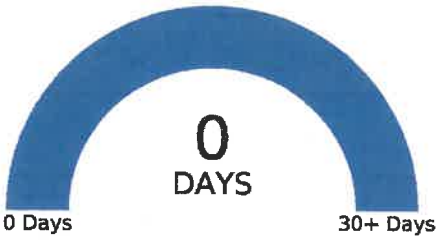
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open Open, No New Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

2023-07-01

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

July 1, 2023 — July 1, 2023
Host Scans on All Addresses

July 1, 2023 — July 1, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

1
Increase of 1
100% of hosts vulnerable

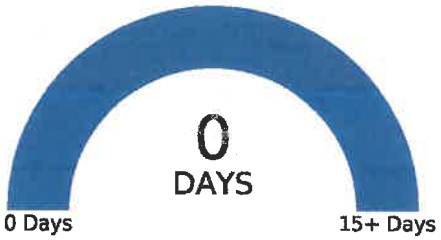
VULNERABILITIES

1
Increase of 1

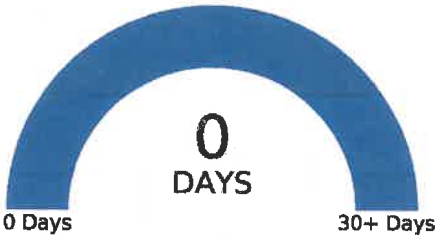
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

2023-06-21

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

June 21, 2023 — June 22, 2023
Host Scans on All Addresses

June 22, 2023 — June 22, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

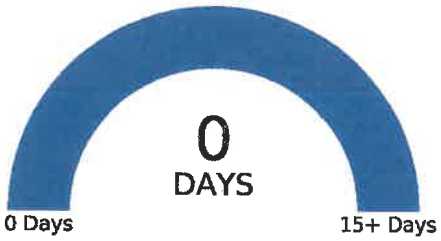
VULNERABILITIES

0
No Change

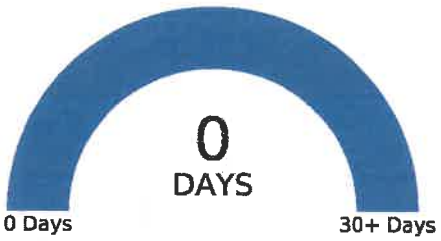
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

2023-06-17

CYBER HYGIENE

REPORT CARD

Skypunch Technology

0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

June 17, 2023 — June 17, 2023
Host Scans on All Addresses

June 17, 2023 — June 17, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

1
No Change

ADDRESSES SCANNED

1
No Change
100% of addresses scanned

HOSTS

1
No Change

SERVICES

2
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

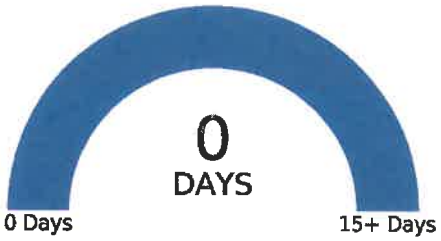
VULNERABILITIES

0
No Change

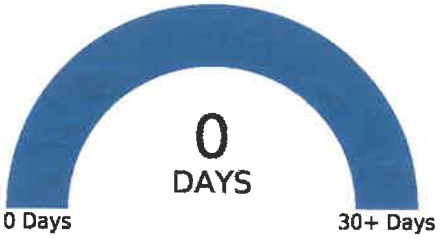
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

Supporting Document

CISA Web Application Scan (WAS)

Skypunch Technology has begun receiving a monthly WAS scan from CISA which is performed using scan technology from Qualys, Burp and Bugcrowd. All of that is heavily centered around OWASP controls. Being a relatively new activity, working with CISA to configure the scanner correctly continues to be a work in progress as it currently scans the site twice when it should be only once and it fails to recognize what CISA has confirmed are false positives. Nevertheless, there is value to be extracted from it and the following report demonstrates where things stand on November 1, 2023 once the confirmed false positives are filtered out.

vulnerability-list-EOIWV

STATUS	NAME	SEVERITY	GROUP	URL	DESCRIPTION	IMPACT
In progress. Apparent false positive.	Passive Mixed Content Vulnerability	1	INFO	https://www.electionsonline.com/vote	Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel.We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images Audio Video	The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests stealing cookies or DOM data leakage.
Resolved	Reflected Cross-Site Scripting (XSS) Vulnerabilities	5	XSS	http://www.electionsonline.com/vote/bios/bio.cfm?candidateID=22131&candidate=%22'%3E%3CqssKflVs8p3%20%60%3b!--%3D%26%7b()%7d%3E	XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text then an attacker can modify the HTML that is received by the victim's Web browser.The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability a malicious user would need to trick a victim into visiting the URL with the XSS payload.	XSS exploits pose a significant threat to a Web application its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently any capability or feature available to the Web browser (for example HTML JavaScript Flash and Java applets) can be used to as a part of a compromise.

STATUS	NAME	SEVERITY	GROUP	URL	DESCRIPTION	IMPACT
In progress. Apparent false positive. Non-verbose error handling is in place sitewide and operable. This is not an injection attempt against an underlying RDBMS, but rather, an attempt to attack the session cookies and their corresponding data in an in-memory data store on the application server which manages state.	Server Error Message	3	INFO	https://www.electionsonline.com/my-account/setup/	This finding will be reported when run time errors verbose server errors and potential stack trace are detected. The following are two examples of 150022 - WAS will send payload without URL encoding and cause an error. Note most browsers now URL encode these payloads in order to reproduce the issue curl or a proxy can help bypass the automatic URL encoding. - Errors can also be caused due to the speed of the scanner sending payloads. The report provides the payload that caused the error if this is consistently reported with SQL payloads it is worth taking an extra look.	Verbose error messages often expose technical details that are helpful to attackers. Verbose errors can allow attackers to learn "inside" information about the application and/or hosting infrastructure allowing them to target it more effectively.
In progress. Apparent false positive. Non-verbose error handling is in place sitewide and operable. This is not an injection attempt against an underlying RDBMS, but rather, an attempt to attack the session cookies and their corresponding data in an in-memory data store on the application server which manages state.	SQL Error Message	2	SQL	https://www.electionsonline.com/my-account/setup/	The scan observed an SQL-based error message while performing injection tests. However the message only appears to indicate that a SQL statement in the web application may be corrupted; it may not be exploitable.SQL injection enables an attacker to modify the syntax of a SQL query in order to retrieve corrupt or delete data. This is accomplished by manipulating query criteria in a manner that affects the query's logic. The typical causes of this vulnerability are lack of input validation and insecure construction of the SQL query.Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. If any part of the string concatenation can be modified then the meaning of the query can be changed.	The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query then the attacker has the equivalent access of a database administrator. This access could lead to theft of data malicious corruption of data or deletion of data.
Resolved	Use of JavaScript Library with Known Vulnerability	3	INFO	https://www.electionsonline.com/online-voting-system/	The web application is using a JavaScript library that is known to contain at least one vulnerability.	Attackers could potentially exploit the vulnerability in the JavaScript library. The impact of a successful exploit depends on the nature of the vulnerability and how the web application makes use of the library.

Supporting Document

Web Application Firewall Managed Rule Groups

Skypunch Technology places a Web Application Firewall (WAF) in front of the entire system. That WAF has enabled four sets of firewall rule groups:

1. Core rule group
2. Known bad inputs rule group
3. SQL database rule group
4. Windows operating system rule group

Each rule group–managed by the experts at Amazon Web Services–contains multiple rules that guard against a wide range of attacks including many of the potential exploitation points provided by OWASP. The following documentation details those rules and provides a description of what it detects and the action taken in response to a detection.

Core rule set (CRS) managed rule group

VendorName: `AWS`, Name: `AWSManagedRulesCommonRuleSet`

The Core rule set (CRS) rule group contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including some of the high risk and commonly occurring vulnerabilities described in OWASP publications such as OWASP Top 10. Consider using this rule group for any AWS WAF use case.

Rule name	Description and label
`NoUserAgent_HEADER`	Inspects for requests that are missing the HTTP `User-Agent` header. Rule action: Block
`UserAgent_BadBots_HEADER`	Inspects for common `User-Agent` header values that indicate that the request is a bad bot. Example patterns include `nessus`, and `nmap`. For bot management, see also AWS WAF Bot Control rule group. Rule action: Block
`SizeRestrictions_QUERYSTRING`	Inspects for URI query strings that are over 2,048 bytes. Rule action: Block
`SizeRestrictions_Cookie_HEADER`	Inspects for cookie headers that are over 10,240 bytes. Rule action: Block
`SizeRestrictions_BODY`	Inspects for request bodies that are over 8 KB (8,192 bytes). Rule action: Block
`SizeRestrictions_URIPATH`	Inspects for URI paths that are over 1,024 bytes. Rule action: Block

`EC2MetaDataSSRF_BODY`	Inspects for attempts to exfiltrate Amazon EC2 metadata from the request body. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block
`EC2MetaDataSSRF_COOKIE`	Inspects for attempts to exfiltrate Amazon EC2 metadata from the request cookie. Rule action: Block
`EC2MetaDataSSRF_URIPATH`	Inspects for attempts to exfiltrate Amazon EC2 metadata from the request URI path. Rule action: Block
`EC2MetaDataSSRF_QUERYARGUMENTS`	Inspects for attempts to exfiltrate Amazon EC2 metadata from the request query arguments. Rule action: Block
`GenericLFI_QUERYARGUMENTS`	Inspects for the presence of Local File Inclusion (LFI) exploits in the query arguments. Examples include path traversal attempts using techniques like `../../`. Rule action: Block
`GenericLFI_URIPATH`	Inspects for the presence of Local File Inclusion (LFI) exploits in the URI path. Examples include path traversal attempts using techniques like `../../`. Rule action: Block

`GenericLFI_BODY`	Inspects for the presence of Local File Inclusion (LFI) exploits in the request body. Examples include path traversal attempts using techniques like `../../`. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block
`RestrictedExtensions_URIPATH`	Inspects for requests whose URI paths contain system file extensions that are unsafe to read or run. Example patterns include extensions like `.log` and `.ini`. Rule action: Block
`RestrictedExtensions_QUERYARGUMENTS`	Inspects for requests whose query arguments contain system file extensions that are unsafe to read or run. Example patterns include extensions like `.log` and `.ini`. Rule action: Block
`GenericRFI_QUERYARGUMENTS`	Inspects the values of all query parameters for attempts to exploit RFI (Remote File Inclusion) in web applications by embedding URLs that contain IPv4 addresses. Examples include patterns like `http://`, `https://`, `ftp://`, `ftps://`, and `file://`, with an IPv4 host header in the exploit attempt. Rule action: Block

`GenericRFI_BODY`	Inspects the request body for attempts to exploit RFI (Remote File Inclusion) in web applications by embedding URLs that contain IPv4 addresses. Examples include patterns like `http://`, `https://`, `ftp://`, `ftps://`, and `file://`, with an IPv4 host header in the exploit attempt. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block
`GenericRFI_URIPATH`	Inspects the URI path for attempts to exploit RFI (Remote File Inclusion) in web applications by embedding URLs that contain IPv4 addresses. Examples include patterns like `http://`, `https://`, `ftp://`, `ftps://`, and `file://`, with an IPv4 host header in the exploit attempt. Rule action: Block
`CrossSiteScripting_COOKIE`	Inspects the values of cookie headers for common cross-site scripting (XSS) patterns using the built-in AWS WAF Cross-site scripting attack rule statement. Example patterns include scripts like `<script>alert("hello")</script>`. **Note** The rule match details in the AWS WAF logs is not populated for version 2.0 of this rule group. Rule action: Block

`CrossSiteScripting_QUERYARGUMENTS`	Inspects the values of query arguments for common cross-site scripting (XSS) patterns using the built-in AWS WAF Cross-site scripting attack rule statement. Example patterns include scripts like `<script>alert("hello")</script>`. **Note** The rule match details in the AWS WAF logs is not populated for version 2.0 of this rule group. Rule action: Block
`CrossSiteScripting_BODY`	Inspects the request body for common cross-site scripting (XSS) patterns using the built-in AWS WAF Cross-site scripting attack rule statement. Example patterns include scripts like `<script>alert("hello")</script>`. **Note** The rule match details in the AWS WAF logs is not populated for version 2.0 of this rule group. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block

`CrossSiteScripting_URIPATH`	Inspects the value of the URI path for common cross-site scripting (XSS) patterns using the built-in AWS WAF Cross-site scripting attack rule statement. Example patterns include scripts like `<script>alert("hello")</script>`. **Note** The rule match details in the AWS WAF logs is not populated for version 2.0 of this rule group. Rule action: Block

Known bad inputs managed rule group

VendorName: AWS, Name: AWSManagedRulesKnownBadInputsRuleSet

The Known bad inputs rule group contains rules to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.

Rule name	Description and label
`JavaDeserializationRCE_HEADER`	Inspects the keys and values of HTTP request headers for patterns indicating Java deserialization Remote Command Execution (RCE) attempts, such as the Spring Core and Cloud Function RCE vulnerabilities (CVE-2022-22963, CVE-2022-22965). Example patterns include `(java.lang.Runtime).getRuntime().exec("whoami")`. **Warning** This rule only inspects the first 8 KB of the request headers or the first 200 headers, whichever limit is reached first, and it uses the `Continue` option for oversize content handling. Rule action: Block

`JavaDeserializationRCE_BODY`	Inspects the request body for patterns indicating Java deserialization Remote Command Execution (RCE) attempts, such as the Spring Core and Cloud Function RCE vulnerabilities (CVE-2022-22963, CVE-2022-22965). Example patterns include `(java.lang.Runtime).getRuntime().exec("whoami")`. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. For more information, see Handling oversize web request components in AWS WAF. Rule action: Block
`JavaDeserializationRCE_URIPATH`	Inspects the request URI for patterns indicating Java deserialization Remote Command Execution (RCE) attempts, such as the Spring Core and Cloud Function RCE vulnerabilities (CVE-2022-22963, CVE-2022-22965). Example patterns include `(java.lang.Runtime).getRuntime().exec("whoami")`. Rule action: Block
`JavaDeserializationRCE_QUERYSTRING`	Inspects the request query string for patterns indicating Java deserialization Remote Command Execution (RCE) attempts, such as the Spring Core and Cloud Function RCE vulnerabilities (CVE-2022-22963, CVE-2022-22965). Example patterns include `(java.lang.Runtime).getRuntime().exec("whoami")`. Rule action: Block

`Host_localhost_HEADER`	Inspects the host header in the request for patterns indicating localhost. Example patterns include `localhost`. Rule action: Block
`PROPFIND_METHOD`	Inspects the HTTP method in the request for `PROPFIND`, which is a method similar to HEAD, but with the extra intention to exfiltrate XML objects. Rule action: Block
`ExploitablePaths_URIPATH`	Inspects the URI path for attempts to access exploitable web application paths. Example patterns include paths like `web-inf`. Rule action: Block
`Log4JRCE_HEADER`	Inspects the keys and values of request headers for the presence of the Log4j vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) and protects against Remote Code Execution (RCE) attempts. Example patterns include `${jndi:ldap://example.com/}`. **Warning** This rule only inspects the first 8 KB of the request headers or the first 200 headers, whichever limit is reached first, and it uses the `Continue` option for oversize content handling. Rule action: Block

`Log4JRCE_QUERYSTRING`	Inspects the query string for the presence of the Log4j vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) and protects against Remote Code Execution (RCE) attempts. Example patterns include `${jndi:ldap://example.com/}`. Rule action: Block
`Log4JRCE_BODY`	Inspects the body for the presence of the Log4j vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) and protects against Remote Code Execution (RCE) attempts. Example patterns include `${jndi:ldap://example.com/}`. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. For more information, see Handling oversize web request components in AWS WAF. Rule action: Block
`Log4JRCE_URIPATH`	Inspects the URI path for the presence of the Log4j vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) and protects against Remote Code Execution (RCE) attempts. Example patterns include `${jndi:ldap://example.com/}`. Rule action: Block

SQL database managed rule group

VendorName: AWS, Name: AWSManagedRulesSQLiRuleSet

The SQL database rule group contains rules to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Evaluate this rule group for use if your application interfaces with an SQL database.

Rule name	Description and label
SQLi_QUERYARGUMENTS	Uses the built-in AWS WAF SQL injection attack rule statement, with sensitivity level set to Low, to inspect the values of all query parameters for patterns that match malicious SQL code. Rule action: Block
SQLiExtendedPatterns_QUERYARGUMENTS	Inspects the values of all query parameters for patterns that match malicious SQL code. The patterns this rule inspects for aren't covered by the rule SQLi_QUERYARGUMENTS. Rule action: Block

`SQLi_BODY`	Uses the built-in AWS WAF SQL injection attack rule statement, with sensitivity level set to Low, to inspect the request body for patterns that match malicious SQL code. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block
`SQLiExtendedPatterns_BODY`	Inspects the request body for patterns that match malicious SQL code. The patterns this rule inspects for aren't covered by the rule `SQLi_BODY`. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block
`SQLi_COOKIE`	Uses the built-in AWS WAF SQL injection attack rule statement, with sensitivity level set to Low, to inspect the request cookie headers for patterns that match malicious SQL code. Rule action: Block

Windows operating system managed rule group

VendorName: AWS, Name: AWSManagedRulesWindowsRuleSet

The Windows operating system rule group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to Windows, like remote execution of PowerShell commands. This can help prevent exploitation of vulnerabilities that permit an attacker to run unauthorized commands or run malicious code. Evaluate this rule group if any part of your application runs on a Windows operating system.

Rule name	Description and label
`WindowsShellCommands_COOKIE`	Inspects the request cookie headers for WindowsShell command injection attempts in web applications. The match patterns represent WindowsShell commands. Example patterns include `||nslookup` and `;cmd`. Rule action: Block
`WindowsShellCommands_QUERYARGUMENTS`	Inspects the values of all query parameters for WindowsShell command injection attempts in web applications. The match patterns represent WindowsShell commands. Example patterns include `|| nslookup` and `;cmd`. Rule action: Block

`WindowsShellCommands_BODY`	Inspects the request body for WindowsShell command injection attempts in web applications. The match patterns represent WindowsShell commands. Example patterns include `||nslookup` and `;cmd`. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block
`PowerShellCommands_COOKIE`	Inspects the request cookie headers for PowerShell command injection attempts in web applications. The match patterns represent PowerShell commands. For example, `Invoke-Expression`. Rule action: Block
`PowerShellCommands_QUERYARGUMENTS`	Inspects the values of all query parameters for PowerShell command injection attempts in web applications. The match patterns represent PowerShell commands. For example, `Invoke-Expression`. Rule action: Block

`PowerShellCommands_BODY`	Inspects the request body for PowerShell command injection attempts in web applications. The match patterns represent PowerShell commands. For example, `Invoke-Expression`. **Warning** This rule only inspects the request body up to the body size limit for the web ACL. The limit is 8 KB for regional web ACLs and 16 KB for CloudFront web ACLs. For CloudFront web ACLs only, you can increase it up to 64 KB in your web ACL configuration. This rule uses the `Continue` option for oversize content handling. Rule action: Block

Supporting Document

Internal Policies

Server Security and Configuration Policies
Details EC2 configuration settings.

Web Application Security Policy
Details development and ongoing monitoring practices for web application security.

SANS

Server Security and Configuration Policy

1. **Overview**
   Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent server installation policies, ownership and configuration management are all about doing the basics well.

2. **Purpose**
   The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Skypunch Technology. Effective implementation of this policy will minimize unauthorized access to Skypunch Technology proprietary information and technology.

3. **Scope**
   All employees, contractors, consultants, temporary and other workers at Skypunch Technology and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Skypunch Technology or registered under a Skypunch Technology-owned internal network domain. This policy specifies requirements for equipment in the Skypunch Technology Virtual Private Cloud (VPC).

4. **General Requirements**
   4.1. All EC2 instances will be registered with and managed by Systems Manager.
   4.2. All EC2 instances used for web-facing applications will be expose to Security Hub and audited against the NIST 800-53 baseline.

2. **Configuration Requirements**

   2.1. Services and applications that will not be used must be disabled where practical.

   2.2. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

   2.3. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

2.4. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

2.5. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

2.6. The server should be configured to set the SameSite attribute as described at https://www.petefreitag.com/item/850.cfm. This should remain in effect until ColdFusion is able to set that attribute on its own.

2.7. Using request filtering, the server should be configured to deny all requests with the exception of those with the following allowable file extensions:

- . (for requests without a file extension)
- .cfc
- .cfm
- .config
- .css
- .dll
- .gif
- .htm
- .html
- .ico
- .jpg
- .js
- .md
- .pdf
- .png
- .txt
- .xml
- .xlsx
- .webp

2.8. The server will include the following response headers:

- X-Content-Type-Options: nosniff
- Strict-Transport-Security: max-age=31536000

- Access-Control-Allow-Origin: https://www.electionsonline.com
- Referrer-Policy: strict-origin-when-cross-origin
- Content-Security-Policy: frame-ancestors 'self' https://www.googletagmanager.com; form-action 'self' https://voter-rosters.s3.amazonaws.com https://skypunch-candidate-photos-source.s3.amazonaws.com; script-src 'unsafe-inline' 'self' https://static.skypunch.tech https://ajax.googleapis.com ajax.googleapis.com https://www.google.com https://www.gstatic.com https://www.googletagmanager.com https://www.google-analytics.com https://cdn.mouseflow.com; style-src 'unsafe-inline' 'self' static.skypunch.tech https://www.gstatic.com; img-src 'self' data: static.skypunch.tech candidates.skypunch.tech www.google.com; media-src 'none'; object-src 'none'; manifest-src 'none'; worker-src 'none'; prefetch-src 'none';
- The server should not send the "Server" response header. Instructions for ensuring this vary from one operating system to the next so it may be necessary to search for instructions over time and across different operating systems.

2.9. The server will be configured to only allow the following HTTP verbs:

- GET
- POST

3. Monitoring

3.1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 week.

5. Policy Compliance

5.1. Compliance Measurement

Skypunch Technology will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by Skypunch Technology management in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

SANS

Web Application Security Policy

1. **Overview**
   Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. **Purpose**
   The purpose of this policy is to define web application security assessments within Skypunch Technology. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Skypunch Technology services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. **Scope**
   This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Skypunch Technology.

   All web application security assessments will be performed by delegated security personnel either employed or contracted by Skypunch Technology. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of Skypunch Technology is strictly prohibited unless approved by management.

   Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. **Policy**
   4.1. Web applications are subject to security assessments based on the following criteria:
      4.1.1. New or Major Application Release – will be subject to a full assessment prior to approval and release into the live environment.
      4.1.2. Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such

time that a proper assessment can be carried out. Emergency releases will be designated as such by an appropriate manager who has been delegated this authority.

4.1.3. Annual Review – all applications will be subject to a full annual review in its entirety to review potential risks of functionality and/or architecture.

4.2. All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

4.2.1. High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment

4.2.2. Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level.

4.2.3. Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3. The following security assessment levels shall be established by Skypunch Technology or other designated organization that will be performing the assessments.

4.3.1. Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

4.3.2. Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

4.3.3. Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4. The current approved web application security assessment tools in use which will be used for testing are:

- Web application scanning as provided by CISA
- Cyber hygiene scanners as provided by CISA
- Manual testing performed internally by those within the Skypunch Technology community along with various Red Team exercises as

executed by cybersecurity students at West Virginia University and West Virginia State University.
- Amazon Inspector

5. **Secure Software Development Lifecycle process**
Skypunch Technology will incorporate security awareness into every phase of software development from planning through maintenance as defined at: https://aws.amazon.com/what-is/sdlc/ under the heading *How does SDLC* work by taking the following steps:
    5.1. During planning, begin by considering where the various attack vectors would be during the development of any new code.
    5.2. During implementation, ensure coders account for identified attack vectors.
    5.3. During development, the first point of reference for any new development activity will always be the OWASP Cheat Series found at https://cheatsheetseries.owasp.org/index.html. Not everything in the the series is applicable to the Skypunch system, but some noteworthy examples that are include:
        5.3.1. Authorization Cheat Sheet
        5.3.2. Authentication Cheat Sheet
        5.3.3. Content Security Policy Cheat Sheet
        5.3.4. Clickjacking Defense Cheat Sheet
        5.3.5. Credential Stuffing Defense Cheat Sheet
        5.3.6. CSRF Cheat Sheet
        5.3.7. Cross Site Scripting Prevention Cheat Sheet
        5.3.8. Database Security Cheat Sheet (Skypunch uses IAM authentication for database authentication which surpasses the recommendations provided here.)
        5.3.9. Error Handling Cheat Sheet
        5.3.10. Forgot Password Cheat Sheet
        5.3.11. File Upload Cheat Sheet
        5.3.12. HTTP Headers Cheat Sheet
        5.3.13. HTTP Strict Transport Security Cheat Sheet
        5.3.14. Insecure Direct Object Reference Prevention Cheat Sheet
        5.3.15. Input Validation Cheat Sheet
        5.3.16. Injection Prevention Cheat Sheet
        5.3.17. Key Management Cheat Sheet (Skypunch handles all key management using AWS KMS making this cheat sheet largely not applicable, but the practices outlined in the cheat sheet are handled natively by KMS.)
        5.3.18. Logging Cheat Sheet
        5.3.19. Multifactor Authentication Cheat Sheet
        5.3.20. Password Storage Cheat Sheet
        5.3.21. Query Parameterization Cheat Sheet
        5.3.22. REST Security Cheat Sheet

5.3.23. Session Management Cheat Sheet
5.3.24. SQL Injection Prevention Cheat Sheet
5.3.25. Secrets Management Cheat Sheet
5.3.26. Transport Layer Protection Cheat Sheet

5.4. Also during implementation, ensure all code is scanned by Amazon Inspector for poor of even vulnerable coding practices as well as current package dependency.

5.5. During testing, attempt to exploit the application by compromising attack vectors. Examples could include, but are not limited to:

5.5.1. SQL injection
5.5.2. Session hijacking
5.5.3. Account impersonation
5.5.4. Et cetera

5.6. Deploy and maintain

6. Policy Compliance

6.1. Compliance Measurement

Skypunch Technology will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

6.2. Exceptions

Any exception to the policy must be approved by Skypunch Technology in advance.

6.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process.Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6. Related Standards, Policies and Processes

OWASP Top Ten Project
OWASP Testing Guide
OWASP Risk Rating Methodology

Supporting Document

Accessibility Conformance Report

Skypunch Technology Accessibility Conformance Report

WCAG Edition

(Based on VPAT® Version 2.4Rev)

Name of Product/Version:

Voting service

Report Date:

September 28, 2023

Product Description:

Web-based voting service.

Contact Information:

David Simms

Notes:

Evaluation Methods Used:

In summer 2022 BeAccessible performed an audit of the voting pages using NVDA with Chrome as the primary screen reader. The website was also manually tested for conformance including and not limited to testing for keyboard-only users, heading levels, color contrast, and system timeout. The scope of that audit was limited to those pages used by voters (the voting pages) plus some parts of the ballot verification wizard which is incorporated into the main website at www.electionsonline.com. The scope did not include all other pages of that main website, nor the election management pages used by election managers to administer elections.

Applicable Standards/Guidelines:

WCAG 2.1

This report covers the degree of conformance for the following accessibility standard/guidelines:

Standard/Guideline	Included In Report
Web Content Accessibility Guidelines 2.0	Level A (No) Level AA (No) Level AAA (No)
Web Content Accessibility Guidelines 2.1	Level A (Yes) Level AA (Yes) Level AAA (No)

Terms

The terms used in the Conformance Level information are defined as follows:

- **Supports**: The functionality of the product has at least one method that meets the criterion without known defects or meets with equivalent facilitation.
- **Partially Supports**: Some functionality of the product does not meet the criterion.
- **Does Not Support**: The majority of product functionality does not meet the criterion.
- **Not Applicable**: The criterion is not relevant to the product.
- **Not Evaluated**: The product has not been evaluated against the criterion. This can be used only in WCAG 2.0 Level AAA.

WCAG 2.x Report

Note: When reporting on conformance with the WCAG 2.x Success Criteria, they are scoped for full pages, complete processes, and accessibility-supported ways of using technology as documented in the WCAG 2.0 Conformance Requirements.

Table 1: Success Criteria, Level A

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.1.1 Non-text Content (Level A)	Supports	
1.2.1 Audio-only and Video-only (Prerecorded) (Level A)	Not applicable	There is no audio-only or video-only content in the system.
1.2.2 Captions (Prerecorded) (Level A)	Not applicable	See above.
1.2.3 Audio Description or Media Alternative (Prerecorded) (Level A)	Not applicable	See above.
1.3.1 Info and Relationships (Level A)	Supports	
1.3.2 Meaningful Sequence (Level A)	Not applicable	There is no occasion where the sequence of page content would ever be different from that when first loaded into the viewer.
1.3.3 Sensory Characteristics (Level A)	Supports	
1.4.1 Use of Color (Level A)	Supports	Color is not used as a navigation aid, but multi-lingual ballots will display text in multiple colors. This was a failed finding when the site was audited by an outside party but resolved during the course of that audit.
1.4.2 Audio Control (Level A)	Not applicable	There is no audio in the system.
2.1.1 Keyboard (Level A)	Supports	
2.1.2 No Keyboard Trap (Level A)	Supports	
2.1.4 Character Key Shortcuts (Level A 2.1 only)	Supports	
2.2.1 Timing Adjustable (Level A)	Supports	
2.2.2 Pause, Stop, Hide (Level A)	Not applicable	There is no moving, blinking, scrolling or auto-updating information as part of the system.
2.3.1 Three Flashes or Below Threshold (Level A)	Supports	
2.4.1 Bypass Blocks (Level A)	Not applicable	The voting pages are very minimal without any repeating elements other than the header on each page.
2.4.2 Page Titled (Level A)	Supports	
2.4.3 Focus Order (Level A)	Supports	
2.4.4 Link Purpose (In Context) (Level A)	Supports	

Criteria	Conformance Level	Remarks and Explanations
2.5.1 Pointer Gestures (Level A 2.1 only)	Supports	It is uncertain if the auditor tested this particular control, but is being marked Supports because there is nothing but very traditional—and typically WCAG-friendly—navigational controls in place throughout the ICT.
2.5.2 Pointer Cancellation (Level A 2.1 only)	Supports	Same as above.
2.5.3 Label in Name (Level A 2.1 only)	Supports	
2.5.4 Motion Actuation (Level A 2.1 only)	Not applicable	There is no motion actuated content as part of the system.
3.1.1 Language of Page (Level A)	Supports	
3.2.1 On Focus (Level A)	Supports	
3.2.2 On Input (Level A)	Supports	
3.3.1 Error Identification (Level A)	Supports	
3.3.2 Labels or Instructions (Level A)	Supports	
4.1.1 Parsing (Level A)	Supports	
4.1.2 Name, Role, Value (Level A)	Supports	

Table 2: Success Criteria, Level AA

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.2.4 Captions (Live) (Level AA)	Not applicable	There is no audio content in the system.
1.2.5 Audio Description (Prerecorded) (Level AA)	Not applicable	See above.
1.3.4 Orientation (Level AA 2.1 only)	Supports	
1.3.5 Identify Input Purpose (Level AA 2.1 only)	Supports	
1.4.3 Contrast (Minimum) (Level AA)	Supports	
1.4.4 Resize text (Level AA)	Supports	
1.4.5 Images of Text (Level AA)	Supports	
1.4.10 Reflow (Level AA 2.1 only)	Supports	
1.4.11 Non-text Contrast (Level AA 2.1 only)	Supports	
1.4.12 Text Spacing (Level AA 2.1 only)	Supports	

Criteria	Conformance Level	Remarks and Explanations
1.4.13 Content on Hover or Focus (Level AA 2.1 only)	Supports	
2.4.5 Multiple Ways (Level AA)	Not applicable	The voting pages employ a wizard interface which voters must navigate through in order.
2.4.6 Headings and Labels (Level AA)	Supports	
2.4.7 Focus Visible (Level AA)	Supports	
3.1.2 Language of Parts (Level AA)	Supports	
3.2.3 Consistent Navigation (Level AA)	Supports	
3.2.4 Consistent Identification (Level AA)	Supports	
3.3.3 Error Suggestion (Level AA)	Supports	
3.3.4 Error Prevention (Legal, Financial, Data) (Level AA)	Supports	
4.1.3 Status Messages (Level AA 2.1 only)	Supports	

Table 3: Success Criteria, Level AAA

Notes: The audit of the Skypunch solution was for compliance with Level AA, therefore the Level AAA table has been removed to truncate this document. It should be noted that much of Level AAA concerns audio which is not applicable to the solution.