TACOMA HOUSING AUTHORITY

RESOLUTION 2021-09-22 (1)

Date: September 22, 2021

To: THA Board of Commissioners

From: April Black
Interim Executive Director

Re: Cybersecurity Policy Approval for NIST 800-171 Compliance

---

This resolution would adopt cybersecurity policies to bring the agency into NIST 800-171 compliance as defined by the Gramm-Leach-Bliley Act of 1999 and required by state and federal agencies.

Background

In order to protect the staff and the community we serve, and to be in compliance with state and federal regulations regarding the protection of personally identifiable information (PII) and other confidential data defined as controlled unclassified information (CUI), the agency should adopt policies to bring THA in compliance with NIST 800-171. NIST 800-171 is a security framework which helps organizations manage and reduce the risk of cybersecurity incidents. The framework was created to operationalize the Gramm-Leach-Bliley Act (GLBA) of 1999. Following the NIST framework as guided by these proposed policies and then by appropriate procedures which operationalize the policies will make THA a safer place in which to work and support our community.

Compliance with NIST 800-171 is required by HUD for any agency dealing with CUI and receiving federal aid and/or grants. While NIST 800-171 audits are not currently common amongst housing authority agencies, compliance would be expected in the event of a breach. And, the federal government, as a whole, is beginning to move towards adoption of the Cybersecurity Maturity Model Certification (CMMC) process as is currently used by the military. Adoption of this standard would require certification that the agency has implemented the NIST framework before federal funding is dispersed.

The agency proposes adopting the proposed policies which would bring THA forward towards compliance with NIST 800-171 and would meet the requirements of CMMC.

While compliance is important and required, the adoption of these policies, the development of supporting procedures and deployment of tactical strategies are first and foremost intended to

make the agency and community safer. For example, when all the tactical statements the policies direct are fully implemented, the THA will not only be much better prepared to fend off attacks from ransomware, phishing attacks, viruses, and the like, but also be in a far better position to respond to these incidents should they occur.

Recommendation

Authorize THA's Executive Director to adopt these proposed NIST 800-171 compliant policies to align the agency with state and federal regulations and requirements.

TACOMA HOUSING AUTHORITY

RESOLUTION 2021-09-22 (1)
(Cybersecurity Policy Approval for NIST 800-171 Compliance)

A **RESOLUTION** of the Board of Commissioners of the Housing Authority of the City of Tacoma

WHEREAS, THA has a vested interest in providing a secure cyber infrastructure for the community it serves and the employees of the agency, and

WHEREAS, NIST 800-171 is a standard cybersecurity framework with operationalizes the Gramm-Leach-Bliley Act of 1999, and

WHEREAS, state and federal agencies are moving to require NIST 800-171 compliance for agencies like THA as a prerequisite for receiving federal funds and grants, and

WHEREAS, the proposed policies bring THA into policy compliance with NIST 800-171, now, therefore, be it

Resolved by the Board of Commissioners of the Housing Authority of the City of Tacoma, Washington as follows:

THA's Executive Director is authorized to adopt policies to bring the agency into NIST 800-171 cybersecurity policy compliance.

Approved: September 22, 2021

Stanley Rumbaugh, Chair

Tacoma Housing Authority

Executive Director
April Black

Board of Commissioners
Stanley Rumbaugh, Chair | Shennetta Smith, Vice Chair
Dr. Minh-Anh Hodge | Derek Young | Pastor Michael Purter

To: Board of Commissioners
From: April Black
Date: 09/01/2021
Subject: Cybersecurity Policies for NIST 800-171 Compliance

Introduction:

The Tacoma Housing Authority (THA) prides itself on being an innovative, Moving to Work (MTW) service organization whose core mission is central to everything it does. In order to protect the staff and the community we serve, and to be in compliance with state and Federal regulations regarding the protection of personally identifiable information (PII) and other confidential data defined as controlled unclassified information (CUI), the agency has moved to adopt policies to bring THA in compliance with NIST 800-171. NIST 800-171 is a security framework which helps organizations manage and reduce the risk of cybersecurity incidents. The framework was created to operationalize the Gramm-Leach-Bliley Act (GLBA) of 1999. Following the NIST framework as guided by these proposed policies and then by appropriate procedures which operationalize the policies will make THA a safer place in which to work and support our community.

Compliance with NIST 800-171 is required by HUD for any agency dealing with CUI and receiving Federal aid and/or grants. While NIST 800-171 audits are not currently common amongst housing authority agencies, compliance would be expected in the event of a breach. However, the Federal government, as a whole, is beginning to move towards adoption of the Cybersecurity Maturity Model Certification (CMMC) process as is currently used by the military. Adoption of this standard would require certification that the agency has implemented the NIST framework before Federal funding is dispersed.

The proposed policies would bring THA forward towards compliance with NIST 800-171 and would meet the requirements of CMMC.

While compliance is important and required, the adoption of these policies, the development of supporting procedures and deployment of tactical strategies are first and foremost intended to make the community safer. For example, when all the tactical statements the policies direct are fully implemented, the THA will not only be much better prepared to fend off attacks from ransomware, phishing attacks, viruses, and the like, but also be in a far better position to respond to these incidents should they occur.

Details:

The following provides a brief summary of each Information Security Policy (ISP) and identifies other stakeholders in the policy, if applicable. Some policies will only impact IT and its practices and be "behind the scenes". For those that do impact end users, the goal is to implement the framework and policies in a way that is compatible with THA workflows, business functionality and mission. In addition, THA is not doing everything as outlined in the policies today. The goal is to bring THA into full compliance over time. These policies are the first step.

- **ISP 01 – Program Management Policy**. THA will develop and maintain an information security program that includes information security policies and procedures. These policies, procedures, and processes are then used to manage, monitor, and support THA's regulatory, legal, risk, environmental, and operational requirements. These requirements are understood and utilized to inform senior leadership of cybersecurity risk. THA will develop and maintain information security policies that have been approved by senior leadership to provide guidance.

  Additional Stakeholder(s): HR, Risk Manager.

- **ISP 02 – Planning Policy.** THA will create and maintain security and privacy plans to manage its systems and data. In addition, THA will provide its staff rules of online behavior and ask them to acknowledge that they understand. Finally, this policy will state that THA will develop a security and privacy architecture to protect the staff and those they serve and that the THA IT unit will be primarily responsible for the development of these plans and architecture.

  Additional Stakeholder(s): HR.

- **ISP 03 – Risk Assessment Policy.** THA will classify its data by risk. THA will periodically conduct assessments of risk, which will include the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification and/or destruction of THA systems, system components, and the information processed, stored, and/or transmitted by the systems. Risk assessment results will be documented and reviewed by the security official or designee. The risk assessment results will then be disseminated to appropriate staff including the THA leadership team. Risk assessments will be conducted annually by THA or whenever there are significant changes to THA, its system, or other conditions that may impact cybersecurity. Finally, THA will monitor and scan its systems for vulnerabilities as part of risk assessment activities.

  Additional Stakeholder(s): Data Standards (PIE), Risk Manager.

- **ISP 04 – Assessment Authorization and Monitoring Policy.** THA will be deliberate in protecting the confidentiality, integrity, and availability of its data and systems and will develop defined plans. THA system, system components, integrations, and assets will be monitored at discrete intervals to identify information security events and to verify the effectiveness of protective measures. THA detection processes and procedures will be maintained to provide for the identification of information security events. Detection processes will be tested and revised to ensure the timely notification of anomalous events to the appropriate responsible parties.

  Additional Stakeholder(s): None.

- **ISP 05 – Supply Chain Management Policy.** THA will be deliberate in its purchasing hardware to ensure that the technology the agency receives has not been compromised, it meets quality/security standards, and that it can get the equipment it needs when it needs it. THA will assess vendors and create contracting standards to ensure THA needs are met. THA will dispose of equipment using secure methods.

  Additional Stakeholder(s): Contracts manager.

- **ISP 06 – System and Service Acquisition Policy.** THA will be deliberate in its purchasing and contracting for software and services. Systems and services will need to be designed and delivered with industry standard security and privacy protections and controls in place. The deployment of systems will be managed with the system lifecycle understood. Vendors will be assessed in how well they meet these requirements.

  Additional Stakeholder(s): Contracts manager.

- **ISP 07 – Identification and Authentication Policy.** THA will limit access to systems, system components, devices, and associated facilities to authorized users, processes, and devices in support of THA's mission and business functions. Multifactor authentication will be deployed for all users. Staff roles and groups will be categorized as to their positional risk with regards to cybersecurity.

  Additional Stakeholder(s): HR.

- **ISP 08 – Access Control Policy.** Access to systems will be actively managed in the use, creation, and deactivation of accounts. Management of accounts will be separated with the creation and deployment managed by different units. Least privilege principles will be applied so staff are given access only to the systems and data they need for their role. Failed attempts to login will be logged. An appropriate use notification will be displayed to users at login. Devices will be locked, and sessions will be terminated after a reasonable defined period of time. Remote access, use of remote devices and WiFi will all actively managed. Information sharing will be controlled.

Additional Stakeholder(s): HR.

- **ISP 09 – Personnel Security Policy.** THA will assign a risk designation to positions and screen employees before hire. THA will remove access to terminated employees and adjust permissions of team members who transfer roles within the organization. There will be access agreements in place for the use of systems. External and/or temporary workers will have security standards they also must meet. Disciplinary procedures will be understood for those who violate these policies. Security and privacy responsibilities, where applicable, will be included in position descriptions.

  Additional Stakeholder(s): HR.

- **ISP 10 – Awareness and Training Policy.** THA staff, and appropriate third-parties will be provided information security awareness training. Appropriate THA staff will be adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, legal requirements, regulations, and agreements. To accomplish this, THA will implement an information security awareness program that discusses common security issues. THA will review the information security awareness program annually and appropriate updates will be applied based on the findings of the annual reviews. THA will require staff to verify annually that they have completed their information security awareness training and are aware of their data security responsibilities and information security policies.

  Additional Stakeholder(s): HR, Risk Manager.

- **ISP 11 – Physical and Environmental Protections Policy.** THA will limit access to specific identified individuals to critical facilities, such as the data center and network closets. Offices will have reasonable controls in place to protect computers while serving guests. Printers will have output controls to prevent unauthorized access and/or use. Access will be monitored. Visitor logs will be kept. Power systems will be protected and include emergency power and lighting capabilities. Emergency shutoff tools for the systems will exist. Fire protection and environmental controls will be functional. Deliveries will be monitored, and unauthorized removal of equipment will be prevented. Remote work sites will be protected. Assets will be tagged, managed, and monitored.

  Additional Stakeholder(s): Facilities.

- **ISP 12 – Maintenance Policy.** THA will perform maintenance on THA systems, system components and any assets providing security functionality to systems and their components. THA acknowledges that proper system maintenance is essential to the performance and availability of THA systems.

  Additional Stakeholder(s): None.

- **ISP 13 – Configuration Management Policy.** THA will develop common standards (baselines) for all deployed systems. It will use change control methodology for the update of these systems, including proactively understanding the security and privacy implications of changes. System changes will be limited to authorized personnel who only have the minimum access they need to accomplish their task. Changes will be documented and a plan to manage changes will be implemented. Systems will be inventoried for their components and software. A data map and architecture will be available where appropriate.

  Additional Stakeholder(s): None.

- **ISP 14 – System and Communications Protections Policy.** THA will separate user functionality from the system management tools. Security infrastructure will prevent the unauthorized transfer of information between systems. THA will take steps to protect systems from denial-of-service actions and ensure necessary resources are available for systems to function properly. THA will secure the boundary between internal and external communications and encrypt data that is transmitted. THA will automatically disconnect network sessions that have been unused for 24 hours. THA will develop and deploy various security standards for remote access and devices. It will use secure standards for network addresses to prevent spoofing. It will have tools that automatically scan for malicious software and actions.

  Additional Stakeholder(s): None.

- **ISP 15 – Media Protection Policy.** THA will protect its digital and non-digital data. Media that contains data will be marked as to whether it is CUI and access will be controlled. If media is transported, it will be secured and protected. If media is disposed of, it will be sanitized. Media will be controlled to prevent its unauthorized removal.

  Additional Stakeholder(s): Facilities.

- **ISP 16 – Data Integrity Policy.** The agency will fix system flaws when they are found and will have tools in place to prevent the injection of malicious code. Systems will be monitored to detect and prevent attacks and otherwise stop unauthorized use of THA systems. The THA will receive and monitor security alerts. Users will be protected from SPAM. System errors will generate useful messages enabling IT staff to correct problems. Data will be maintained according to applicable laws and regulations. Data will be monitored for accuracy and data that is shared will be de-identified as appropriate.

  Additional Stakeholder(s): Data standards (PIE).

- **ISP 17 – Audit and Accountability Policy.** THA systems will log events meaningfully and will be stored for a reasonable amount of time as required by law and regulations. If logging fails, the IT team will be notified. Logs will be regularly reviewed for anomalies and to detect unauthorized use of THA systems. Logs will be in a state that is usable by the IT team. Logs will be protected and secured from tampering or other unauthorized access. Tools will be in place to notify the IT team of significant events.

  Additional Stakeholder(s): None.

- **ISP 18 – Incident Response Policy.** THA will have an Incident Response Plan (IRP) that addresses the processes and procedures to be executed and maintained, to ensure timely response to a detected information security event. Analysis of detected information security events will be conducted to ensure adequate response and to support recovery activities. Upon detection of an information security event, THA will take the necessary actions, including calling on external resources, to prevent the expansion of an event, to mitigate its effects, and eradicate the incident. Upon mitigation of an information security event, THA will incorporate lessons learned into the IRP to improve upon it and report as legally required.

  Additional Stakeholder(s): Risk Manager.

- **ISP 19 – Contingency Planning Policy.** THA will identify critical systems and develop plans to continue its mission in the event of an emergency. The agency will train on these plans in order to execute them effectively and test to ensure the plans are actually effective. It will use cloud services where applicable to provide for business continuity. THA will develop alternative paths for communications as a backup strategy to keep the agency online and functioning. THA will back up its systems where appropriate and will test those backups routinely to ensure they provide the protection intended.

  Additional Stakeholder(s): Risk Manager.

- **ISP 20 – Data Privacy Policy.** THA will alert the public to its privacy policies. It will have processes and procedures in place to ensure the accuracy and integrity of its collected data. THA will reasonably restrict access to private information to the greatest extent possible including for internal use. THA will have mechanisms in place to deal with privacy concerns including contact information on our website. Privacy will be considered in the development of THA systems and people will be asked to consent for the use of their data.

  Additional Stakeholder(s): Communications, HR.