INTERCONNECTION SECURITY AGREEMENT BETWEEN NIST AND iEdison ORGANIZATIONS

Table of Contents

Introduction

A system interconnection is defined as the direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources. The associated security control within the NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations,* primarily refers to connections but uses the terms connections and interconnections interchangeably. An interconnection security agreement (ISA) is used to document connections between systems. The ISA is more than a contract or service agreement between two agencies, departments, divisions, external entities; the ISA is a security agreement that protects both interconnected systems. NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems states the intent behind an ISA is to detail some basic system information and then to document and agree on how the security of the two systems will be maintained. Significant benefits that can be realized through a system connection include reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting IT systems may also strengthen ties among participating organizations by promoting communication and cooperation.

This ISA applies to users of iEdison – institutions, private companies, other Federal agencies – that plan to use the iEdison Application Programming Interface (API).

Information Sensitivity

The iEdison System has a security categorization and impact rating of Moderate for Confidentiality and Integrity, and Low for Availability. The security classification of the iEdison users' systems that will be connecting to iEdison could range from Low to Moderate. All sensitive data exchanged between iEdison and the other systems will be treated as Controlled Unclassified Information (CUI) and must be kept confidential in accordance with 35 USC 205, 37 CFR 401.13(c), and other applicable Federal laws and regulations.

The design and implementation for the connected applications will determine the specifics of what security controls can be inherited or shared. The infrastructure and applications are sufficiently segregated to ensure that vulnerabilities could not be exploited between iEdison and the connecting systems.

All users and administrators are expected to protect the information transmitted in accordance with all required Federal laws, regulations, and NIST guidance.

System Vulnerabilities

Vulnerabilities in interconnected systems can have an adverse impact on the security of all parties. Because of this, the system owners and the security officers must be aware of the identified vulnerabilities of all the systems that are connected to their system(s). Report any identified security incidents affecting the systems interconnecting with iEdison through the use/inquiry form (https://nistgov.force.com/iedison). For purposes of this ISA, a security incident is defined as a substantiated threat of, compromise including, but not limited to unauthorized destruction, access, disclosure, use and/or alteration, or a risk to the system's environment or operations.

At the time of entering into this ISA, the current Plan of Action and Milestones (POA&M) for iEdison can be located by contacting the relevant IT Security Officer at NIST (helen.nelson@nist.gov). Special attention should be paid to any moderate, high and critical severity level vulnerabilities. For these levels of vulnerabilities, the system owners for the affected systems agree to work with each other.

The Department of Commerce (DoC) has created a Vulnerability Disclosure Policy (VDP) and Vulnerability Disclosure Program (https://www.commerce.gov/vulnerability-disclosure-policy), to give security researchers clear guidelines for performing vulnerability discovery activities on DoC systems and websites, as well as to convey DoC's preferences in how to submit discovered vulnerabilities to DoC. DoC's VDP applies to the iEdison system, and as such, active research and testing will be conducted on the application as stipulated in the DoC policy, including abiding to agree by vulnerability reporting requirements as set forth in the policy.

Information Exchange Security

All data is encrypted at rest and in transit using FIPS 140-2 or FIPS 140-3 validated encryption. The connections at each end are located within controlled access facilities, guarded 24 hours a day. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

Incident Reporting

The party discovering a security incident will report it in accordance with its incident reporting procedures.

NIST reserves the right to disconnect any user that poses a security (or any other) threat to the agency or other customers in consultation with the NIST System Owner/designee, NIST CIO/designee, and as reported to the Security Implementation and Incident Response Team (SIIRT, siirt@nist.gov) and the iEdison Support Team (https://www.nist.gov/iedison).

Each organization will keep NIST informed in writing through their respective Information System Security Officer(s) (ISSO) when security incidents occur which might have any impact on the other organization's systems. These information exchanges will take place as soon as practical to ensure that appropriate steps are immediately taken to mitigate any potential loss/compromise of data or denial of service.

Backups/Updates/Changes

iEdison data is stored on NIST servers and backed up using Amazon Web Services (AWS) components. Formal change management procedures are followed for NIST servers and databases. Backups and system changes will be handled per agreed-upon procedures documented for the system.

Planned technical updates and changes to the system architecture expected to impact users will be reported and communicated by NIST to iEdison users before such changes are implemented. If any of the technical changes significantly impact the security of the iEdison system, NIST will conduct a risk assessment based on the new system architecture, modify, and re-sign the ISA as soon as practical. If a new unapproved interconnection, interface, and/or service is detected, it will be refused and documented as a possible intrusion until authorized.

Rules of Behavior

Any new or additional security awareness or training requirements, which may include additional agreements, can be developed (and required to be satisfied) as needed, mainly due to the interconnections between the iEdison system and the users' systems.

All users and administrators are expected to protect the information transmitted in accordance with all required laws, regulations, and NIST guidance.

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit. Each party represents that its respective system is designed, managed, and operated in compliance with all relevant agency regulations, official guidance, and policies.

Audit Trail Responsibilities

The organizations shall implement audit and accountability policies and procedures as required by Federal guidance (i.e., Federal Information Processing Standard (FIPS) 200, Executive Order 14028, and OMB M-21-31) for proactive and post-incident response efforts.

Overall IT Security Posture of Organizations

Each organization will ensure that any third-party entities (vendors or private companies) that they choose to act on their behalf to connect to iEdison, work on the iEdison connection, or work on systems connected to iEdison, have gone through appropriate independent IT security assessments, in accordance with relevant Federal legal authority (Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB), NIST Special Publications, etc.). As the decision to work with a third party is made by (and at the discretion of) the organization (which could be a Federal entity), the responsibility in ensuring that the third party or vendor to connect to iEdison, work on the iEdison connection, or work on systems connected to iEdison, meets all Federal security requirements rests with the organization. In addition, the organization will notify NIST when its vendor's IT architecture goes through a significant change[1].

NIST reserves the right to request, and each organization agrees to provide, documentation, including vulnerability scan results and other potentially proprietary data, related to any third party's IT security posture at any point during that organization's interconnection period with the iEdison system, particularly during NIST's IT security annual continuous monitoring activities.

As reference, the following Federal security regulations are deemed relevant:

- Federal Information Security Management Act (FISMA) of 2014, Public Law 113-283;
- Office of Management and Budget, Circular No. A-130, Managing Information as a Strategic Resource;
- Office of Management and Budget, Circular No. A-123, Management's Responsibility for Internal Controls;
- Office of Management and Budget, Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publications under the Privacy Act;
- NIST Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations;
- NIST Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy;
- Federal Information Processing Standards Publication (FIPS PUB) 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Federal Information Processing Standards Publication (FIPS PUB) 200, Minimum Security Requirements for Federal Information and Information Systems

[1] A significant change is one that is likely to affect the security state of the information system or IT environment/infrastructure.

Signatory Authority

This ISA is valid for three (3) years after the last date on either signature below. At that time it will be updated, reviewed, and reauthorized. Any participating party may terminate this agreement upon 30 days' advanced written notice to NIST or in the event of a security incident that necessitates an immediate response.

National Institute of Standards and Technology (NIST):

CHIHMING HUANG Digitally signed by CHIHMING HUANG Date: 2024.11.19 14:32:51 -05'00'

Chihming (Richard) Huang, iEdison System Owner Date

HANNAH BROWN Digitally signed by HANNAH BROWN Date: 2024.11.20 07:59:13 -05'00'

Hannah Brown (NIST Chief Information Officer) ***or*** Date
Blair Heiserman (NIST Chief Information Security Officer)

Agency/Institution/Organization:

Name and Title Date

Name and Title Date

Name and Title Date