



Securing SUNY

May 12th, 2020

Kevin T Stillman

Director, Network & Cybersecurity Services

SUNY System Administration

www.suny.edu





The State University
of New York

Security Landscape

Within the last 12 months SUNY Campuses alone have reported to SUNY CISO:

- 1 ransomware attack that crippled a campus for several days during registration
- 2 less successful ransomware attacks, but required days by IT staff to remediate
- 1 sextortion attempt
- 5 instances of data breach of more than 100 records
- Dozens of instances of Directed Denial of Service attacks that have crippled campus services
- Dozens of targeted Phishing attacks intended to fool the target into taking an action

And these are only the incidents that have been reported...





The State University
of New York

Security Landscape

What are they after?

- Money – Higher Ed is a soft target
- Intellectual Property – Especially at research institutions
- State sponsored attacks for political ends China, Russia, Iran (Soleimani death), North Korea conflict
- Identity theft of students, faculty and staff
- Disruption of the institution from disgruntled student, employee, or other

So what's a 64 Campus University System to do?



Create Policies & Procedures... Of course!

2003	New York State issued its Information Security Policy SUNY reacted and began developing its strategy
2003	Information Security Officers defined at SUNY System Administration and some campuses
2005	Cyber-incident reporting process was established based on NYS's policies
2005	System Administration's ISO became SUNY CISO

2007	SUNY Board Procedure 6608 established baseline Information Security program requirements for State Operated campus: <ul style="list-style-type: none"> • Information Security controls based on CIS 20 Critical Controls • Campuses required to complete annual SAQ (self-assessment questionnaire) to report compliance status
2011	<ul style="list-style-type: none"> • SAQ was split to include both IT Controls and Information Security Management • Information Security Management framework based on ISO 27001

2015	The SUNY SOC Program was established to provide uniform cyber-security services to participating SUNY campuses
2016	SUNY Board Policy 6900 expanded Procedure 6608's scope: <ul style="list-style-type: none"> • 6608 was expanded to include Community Colleges • Campuses Presidents officially accountable for compliance • Annual Information Security Awareness training requirements added • Re-affirmed cyber incident reporting procedures initially established in 2005

And Now... The SUNY NIST Policy Initiative

- The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the U.S. Commerce Department.
- The NIST 800-53 standards are a comprehensive catalogue of cybersecurity controls and implementation guidelines for information systems.
- The Chancellor’s Executive Leadership team has approved the adoption of policies based on the NIST 800-53 security controls.
- These policies were adopted on 1/1/20 with an effective date of 1/1/22 to allow for a 2 year implementation window.

NIST the Emerging Standard	Chancellor’s Initiatives	Enhance Current Cybersecurity Efforts	Campus Interest
<p>Federal</p> <ul style="list-style-type: none"> • Mandated for all Federal agencies, including the Department of Education and Title IV/Financial Aid • Will be required for the Single Audit <p>State</p> <ul style="list-style-type: none"> • 800-53 satisfies all NYS ITS recommended security controls • Other states governments are adopting these standards: TX, CA • Major private universities are also adopting the standards. <p>Higher Ed</p> <ul style="list-style-type: none"> • Other major university systems have adopted the NIST Standards: UC, UT, Illinois, Wisconsin 	<p>SUNY Online</p> <ul style="list-style-type: none"> • Cybersecurity becomes more important as we move to a centralized cloud-based platform. Having uniform policies is one way to ensure that this cloud-based environment is secure. • Including cybersecurity as part of the SUNY Online process is efficient and logical. <p>Federal Research Grants</p> <ul style="list-style-type: none"> • Satisfies mandated information security requirements for federal research grants 	<p>Current Cybersecurity Efforts</p> <ul style="list-style-type: none"> • Annual completion of self-assessment questionnaire • Membership in the Security Operations Center (SOC) <p>Limitations</p> <ul style="list-style-type: none"> • The responses to the assessments are subjective; metrics are not strictly defined; subjective responses are not comparable; results do not provide reasonable assurance that risks are being mitigated • Membership in the SOC is optional, and utilization of services is low <p>Benefits</p> <ul style="list-style-type: none"> • The polices provide process, structure, and well-defined, articulated requirements. • Standardized cybersecurity requirements will enhance monitoring and assessment capability 	<p>Survey Results</p> <ul style="list-style-type: none"> • 2018 campus survey indicates that campuses want assistance with information security policy development and best practices • Over 70% of responding campuses indicated this is needed or strongly needed • Almost 70% indicated they needed or strongly needed help with NIST expertise. • Just over 50% indicated a strong need or need for Information Security as a service



The State University
of New York

SUNY's NIST Framework Adoption

- NIST 800-53 Low Baseline Implementation
 - SUNY has adopted 17 policies based on control families
 - Implementing **115 Controls**
 - The controls are to be rolled out in Four 6-month long phases
- Policies are standardized for uniformity
- Each Policy addresses Purpose, Scope, Compliance and Guidance
- Provides a framework for campuses to align their controls and advocate for resources
- Creates consistency across the System





115 Controls to adopt

Control Number	Control Name	Priority	Initial Control Baselines
			LOW
Access Control			
AC-1	Access Control Policy and Procedures	P1	AC-1
AC-2	Account Management	P1	AC-2
AC-3	Access Enforcement	P1	AC-3
AC-7	Unsuccessful Logon Attempts	P2	AC-7
AC-8	System Use Notification	P1	AC-8
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14
AC-17	Remote Access	P1	AC-17
AC-18	Wireless Access	P1	AC-18
AC-19	Access Control for Mobile Devices	P1	AC-19
AC-20	Use of External Information Systems	P1	AC-20
AC-22	Publicly Accessible Content	P3	AC-22
Awareness and Training			
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1
AT-2	Security Awareness Training	P1	AT-2
AT-3	Role-Based Security Training	P1	AT-3
AT-4	Security Training Records	P3	AT-4
Audit and Accountability			
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1
AU-2	Audit Events	P1	AU-2
AU-3	Content of Audit Records	P1	AU-3
AU-4	Audit Storage Capacity	P1	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6
AU-8	Time Stamps	P1	AU-8
AU-9	Protection of Audit Information	P1	AU-9
AU-11	Audit Record Retention	P3	AU-11
AU-12	Audit Generation	P1	AU-12

Control Number	Control Name	Priority	Initial Control Baselines
			LOW
Security Assessment and Authorization			
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1
CA-2	Security Assessments	P2	CA-2
CA-3	System Interconnections	P1	CA-3
CA-5	Plan of Action and Milestones	P3	CA-5
CA-6	Security Authorization	P2	CA-6
CA-7	Continuous Monitoring	P2	CA-7
CA-9	Internal System Connections	P2	CA-9
Configuration Management			
CM-1	Configuration Management Policy and Procedures	P1	CM-1
CM-2	Baseline Configuration	P1	CM-2
CM-4	Security Impact Analysis	P2	CM-4
CM-6	Configuration Settings	P1	CM-6
CM-7	Least Functionality	P1	CM-7
CM-8	Information System Component Inventory	P1	CM-8
CM-10	Software Usage Restrictions	P2	CM-10
CM-11	User-Installed Software	P1	CM-11
Contingency Planning			
CP-1	Contingency Planning Policy and Procedures	P1	CP-1
CP-2	Contingency Plan	P1	CP-2
CP-3	Contingency Training	P2	CP-3
CP-4	Contingency Plan Testing	P2	CP-4
CP-9	Information System Backup	P1	CP-9
CP-10	Information System Recovery and Reconstitution	P1	CP-10
Identification and Authentication			
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)
IA-4	Identifier Management	P1	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)
IA-6	Authenticator Feedback	P2	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7
IA-8	Identification and Authentication (Non-Organizational)	P1	IA-8 (1) (2) (3) (4)





And more controls...

Control Number	Control Name	Priority	Initial Control Baselines LOW
	Users)		
Incident Response			
IR-1	Incident Response Policy and Procedures	P1	IR-1
IR-2	Incident Response Training	P2	IR-2
IR-4	Incident Handling	P1	IR-4
IR-5	Incident Monitoring	P1	IR-5
IR-6	Incident Reporting	P1	IR-6
IR-7	Incident Response Assistance	P2	IR-7
IR-8	Incident Response Plan	P1	IR-8
Maintenance			
MA-1	System Maintenance Policy and Procedures	P1	MA-1
MA-2	Controlled Maintenance	P2	MA-2
MA-4	Nonlocal Maintenance	P2	MA-4
MA-5	Maintenance Personnel	P2	MA-5
Media Protection			
MP-1	Media Protection Policy and Procedures	P1	MP-1
MP-2	Media Access	P1	MP-2
MP-6	Media Sanitization	P1	MP-6
MP-7	Media Use	P1	MP-7
Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2
PE-3	Physical Access Control	P1	PE-3
PE-6	Monitoring Physical Access	P1	PE-6
PE-8	Visitor Access Records	P3	PE-8
PE-12	Emergency Lighting	P1	PE-12
PE-13	Fire Protection	P1	PE-13
PE-14	Temperature and Humidity Controls	P1	PE-14
PE-15	Water Damage Protection	P1	PE-15
PE-16	Delivery and Removal	P2	PE-16

Control Number	Control Name	Priority	Initial Control Baselines LOW
Planning			
PL-1	Security Planning Policy and Procedures	P1	PL-1
PL-2	System Security Plan	P1	PL-2
PL-4	Rules of Behavior	P2	PL-4
Personnel Security			
PS-1	Personnel Security Policy and Procedures	P1	PS-1
PS-2	Position Risk Designation	P1	PS-2
PS-3	Personnel Screening	P1	PS-3
PS-4	Personnel Termination	P1	PS-4
PS-5	Personnel Transfer	P2	PS-5
PS-6	Access Agreements	P3	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7
PS-8	Personnel Sanctions	P3	PS-8
Risk Assessment			
RA-1	Risk Assessment Policy and Procedures	P1	RA-1
RA-2	Security Categorization	P1	RA-2
RA-3	Risk Assessment	P1	RA-3
RA-5	Vulnerability Scanning	P1	RA-5
System and Services Acquisition			
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1
SA-2	Allocation of Resources	P1	SA-2
SA-3	System Development Life Cycle	P1	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)
SA-5	Information System Documentation	P2	SA-5
SA-9	External Information System Services	P1	SA-9
System and Communications Protection			
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1
SC-5	Denial of Service Protection	P1	SC-5
SC-7	Boundary Protection	P1	SC-7
SC-12	Cryptographic Key Establishment and Management	P1	SC-12
SC-13	Cryptographic Protection	P1	SC-13
SC-15	Collaborative Computing Devices	P1	SC-15





And still more controls...

Control Number	Control Name	Priority	Initial Control Baselines
			LOW
RA-5	Vulnerability Scanning	P1	RA-5
System and Services Acquisition			
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1
SA-2	Allocation of Resources	P1	SA-2
SA-3	System Development Life Cycle	P1	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)
SA-5	Information System Documentation	P2	SA-5
SA-9	External Information System Services	P1	SA-9
System and Communications Protection			
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1
SC-5	Denial of Service Protection	P1	SC-5
SC-7	Boundary Protection	P1	SC-7
SC-12	Cryptographic Key Establishment and Management	P1	SC-12
SC-13	Cryptographic Protection	P1	SC-13
SC-15	Collaborative Computing Devices	P1	SC-15
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22
SC-39	Process Isolation	P1	SC-39
System and Information Integrity			
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1
SI-2	Flaw Remediation	P1	SI-2
SI-3	Malicious Code Protection	P1	SI-3
SI-4	Information System Monitoring	P1	SI-4
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5
SI-12	Information Handling and Retention	P2	SI-12
Total Number of Controls			115



System Admin's NIST Framework Adoption

- Seems extraordinarily daunting, BUT...
- Milestones are:
 - Phase 1 – 33 Controls to be complete by July 1, 2020
 - Phase 2 - 66 Controls to be complete by January 1, 2021
 - Phase 3 – 92 Controls to be complete by July 1, 2021
 - Phase 4 – 115 Total Controls to be complete by January 1, 2022
 - *That's 4.8 Controls a month... we can swing that*
- Much of what are in the policies are most likely already being done, or partially done, by the various IT or Business groups as standard practice. (not documented)
- AND, the Controls are already written as templates, we just need to adapt.
- **Divide and conquer as a team** is the best way to proceed!

System Admin's NIST Framework Adoption

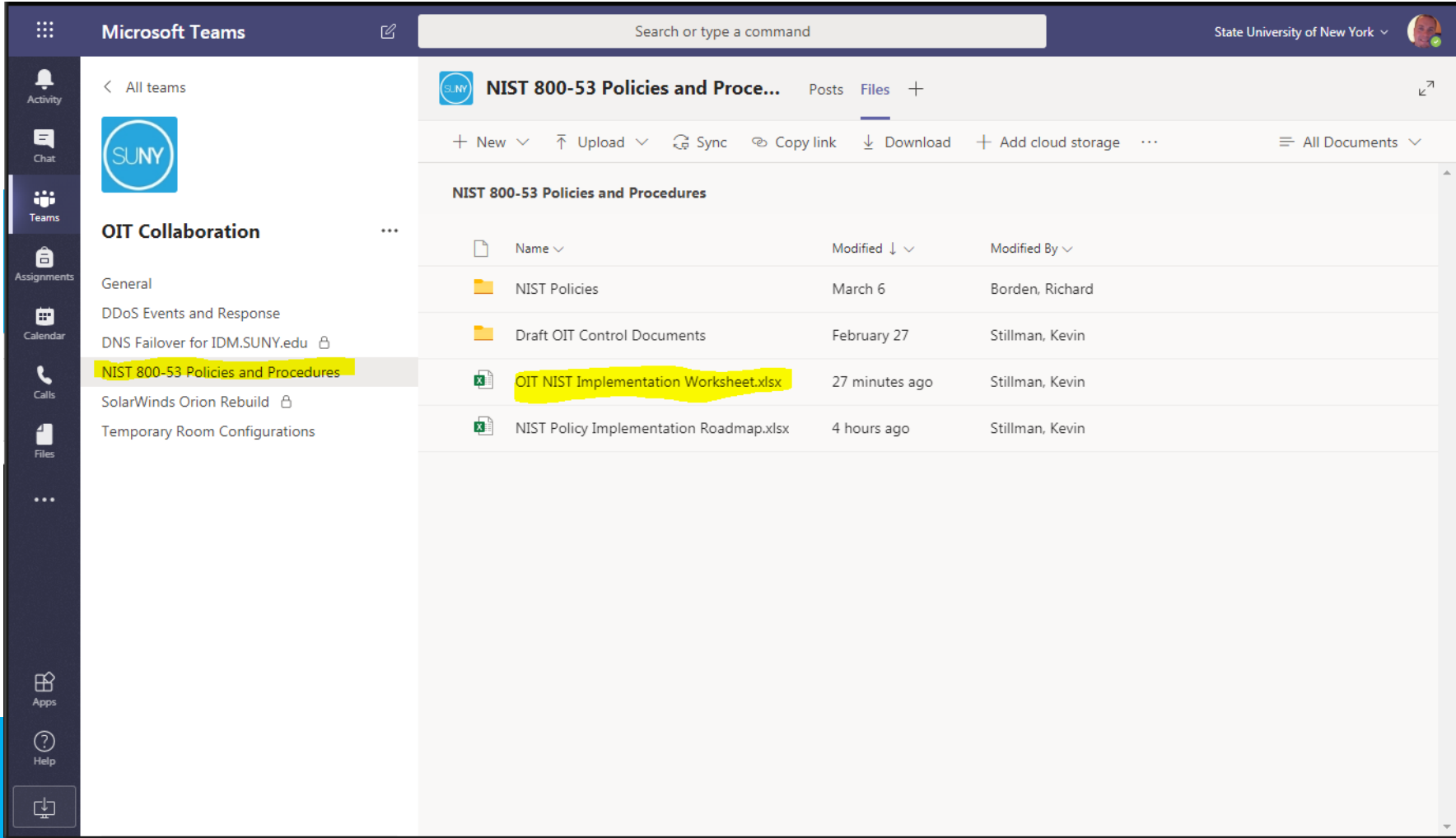
Server Infrastructure

Middleware

Help Desk

Database

Desktop Support



The screenshot shows a Microsoft Teams interface for a team named 'OIT Collaboration'. The 'Files' tab is active, displaying a list of documents under the folder 'NIST 800-53 Policies and Procedures'. The file 'OIT NIST Implementation Worksheet.xlsx' is highlighted in yellow. The interface includes a search bar at the top, a navigation pane on the left with icons for Activity, Chat, Teams, Assignments, Calendar, Calls, Files, and Help, and a user profile in the top right corner.

Name	Modified	Modified By
NIST Policies	March 6	Borden, Richard
Draft OIT Control Documents	February 27	Stillman, Kevin
OIT NIST Implementation Worksheet.xlsx	27 minutes ago	Stillman, Kevin
NIST Policy Implementation Roadmap.xlsx	4 hours ago	Stillman, Kevin

Networking

IT Security

Development

Production Control

IT Leadership



AC-17

REMOTE ACCESS

Process Owner	Kevin Stillman / John Green
Process Operator	Network Operations / Help Desk
Occurrence	Ongoing
Scope of Impact	Continually occurring in the background
Additional Documentation	
Performance Target	N/A
Technology in Use	Pulse VPN Appliance, Guacamole, Domain Controllers, Microsoft MFA
Technical Summary	Remote access is delivered to remote employees and contractors via a Pulse VPN appliance and Guacamole server remote access. Help Desk installs VPN client software for SUNY-owned devices. Standard User devices access a VPN network segment that has the same access as a standard user network. IT Operations staff access a network segment that can access management interfaces of IT infrastructure. Employees with non-SUNY devices that are allowed to use VPN do not connect directly to a network segment but are only allowed to Remote Desktop to a secure device on the network. Access is controlled via groups in the domain controller and are assigned by the Help Desk.

Control Objective: The organization: ¹

- Documents allowed methods of remote access to systems;
- Establishes usage restrictions and implementation guidance for each allowed remote access method;
- Monitors for unauthorized remote access to systems;
- Authorizes remote access to the system prior to connection; and
- Enforces requirements for remote connections to systems.

Control: Mechanisms exist to define, control and review remote access methods.

Procedure / Control Activity: Systems Security Developer [SP-SYS-001], in conjunction with Security Architect [SP-ARC-002], Systems Security Manager [OV-MGT-001] and Network Operations Specialist [OM-NET-001]:

- (1) Uses industry-recognized practices to develop a defense-in-depth approach to protecting the network and SUNY System Administration's data.
- (2) Uses vendor-recommended settings and industry-recognized secure practices to implement remote access, in accordance with SUNY System Administration policies and standards, as follows:
 - a. Document allowed methods of remote access to the information system;
 - b. Establish usage restrictions and implementation guidance for each allowed remote access method;
 - c. Monitor for unauthorized remote access to information systems;
 - d. Authorize remote access to information systems prior to connection;
 - e. Enforce requirements for remote connections to information systems;
 - f. Use cryptography to protect the confidentiality and integrity of remote access sessions;
 - g. Automatically disconnect remote access sessions after a period of inactivity; and
 - h. Immediately deactivate vendor and business partner remote access when it is no longer needed.

¹ NIST 800-53 rev4 AC-17 | ISO 27002 6.2.2 | FedRAMP | NIST 800-171 3.1.1 & 3.1.2 | PCI DSS 12.3.8 & 12.3.9 | NIST CSF PR.AC-3 | CSC 12.7

System Admin's NIST Framework Adoption

A	B	C	D	E	F
Phase	Control Family	Control Number	Control Name	Reviewer(s)	Status
P1	Access Control	AC-1	Access Control Policy and Procedures	Kevin / All	Kevin started. All should review.
P1	Access Control	AC-17	Remote Access	Kevin / John	Kevin started. John should review the Help Desk sections
P1	Access Control	AC-18	Wireless Access	Kevin / John	Kevin started. John should review the Help Desk sections
P1	Access Control	AC-19	Access Control for Mobile Devices	John	Kevin added the table. John should review.
P1	Access Control	AC-2	Account Management	Jim / John / Kevin	This one has a lot in it. Needs discussion
P1	Access Control	AC-20	Use of External Information Systems	All	This one needs discussion
P1	Access Control	AC-3	Access Enforcement	Jim	Jim should review this. Varonis does this for FD/One Drive. What about applications?
P1	Access Control	AC-8	System Use Notification	All	Kevin started. Others should review and consider
P1	Awareness and Training	AT-1	Security Awareness and Training Policy and Procedures	Ken	
P1	Awareness and Training	AT-2	Security Awareness Training	Ken	
P1	Awareness and Training	AT-3	Role-Based Security Training	Ken	
P1	Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures	Kevin	Completed. Needs Review
P1	Audit and Accountability	AU-12	Audit Generation	Kevin	Completed. Needs Review
P1	Audit and Accountability	AU-2,6	Audit Events	Kevin	Completed. Needs Review
P1	Audit and Accountability	AU-3	Content of Audit Records	Ken	
P1	Audit and Accountability	AU-4	Audit Storage Capacity	Ken	
P1	Audit and Accountability	AU-5	Response to Audit Processing Failures	Ken	
P1	Audit and Accountability	AU-8	Time Stamps	Ken	
P1	Audit and Accountability	AU-9	Protection of Audit Information	Ken	
P1	Security Assessment and Authorization	CA-1	Security Assessment and Authorization Policies and Procedures	Kevin / Jim	
P1	Security Assessment and Authorization	CA-3	System Interconnections	Kevin / Jim	Needs discussion. Seems impractical with virtualization
P1	Configuration Management	CM-1	Configuration Management Policy and Procedures	Jim / John / Kevin	
P1	Configuration Management	CM-11	User-Installed Software	Jim / John / Kevin	
P1	Configuration Management	CM-2,6	System Hardening Through Baseline Configurations	Jim / John / Kevin	
P1	Configuration Management	CM-7	Least Functionality	Jim / John / Kevin	
P1	Configuration Management	CM-8	Information System Component Inventory	Jim / John / Kevin	
P1	Contingency Planning	CP-1,2	Contingency Plan Update	All	
P1	Contingency Planning	CP-10	Information System Recovery and Reconstitution	All	
P1	Contingency Planning	CP-9	Information System Backup	All	
P1	Identification and Authentication	IA-1	Identification and Authentication Policy and Procedures	Jim / John / Kevin	
P1	Identification and Authentication	IA-2	Identification and Authentication (Organizational Users)	Jim / John / Kevin	
P1	Identification and Authentication	IA-4	Identifier Management	Jim / John / Kevin	
P1	Identification and Authentication	IA-5	Authenticator Management	Jim / John / Kevin	
P1	Identification and Authentication	IA-7	Cryptographic Module Authentication	Jim / John / Kevin	

A	B	C	D	E	F
Phase	Control Family	Control Number	Control Name	Reviewer(s)	Status
P1	Access Control	AC-1	Access Control Policy and Procedures	Kevin / All	Kevin started. All should review.
P1	Access Control	AC-17	Remote Access	Kevin / John	Kevin started. John should review the Help Desk sections
P1	Access Control	AC-18	Wireless Access	Kevin / John	Kevin started. John should review the Help Desk sections
P1	Access Control	AC-19	Access Control for Mobile Devices	John	Kevin added the table. John should review.
P1	Access Control	AC-2	Account Management	Jim / John / Kevin	This one has a lot in it. Needs discussion
P1	Access Control	AC-20	Use of External Information Systems	All	This one needs discussion
P1	Access Control	AC-3	Access Enforcement	Jim	Jim should review this. Varonis does this for FD/One Drive. What about applications?
P1	Access Control	AC-8	System Use Notification	All	Kevin started. Others should review and consider
P1	Awareness and Training	AT-1	Security Awareness and Training Policy and Procedures	Ken	
P1	Awareness and Training	AT-2	Security Awareness Training	Ken	
P1	Awareness and Training	AT-3	Role-Based Security Training	Ken	
P1	Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures	Kevin	Completed. Needs Review
P1	Audit and Accountability	AU-12	Audit Generation	Kevin	Completed. Needs Review
P1	Audit and Accountability	AU-2,6	Audit Events	Kevin	Completed. Needs Review
P1	Audit and Accountability	AU-3	Content of Audit Records	Ken	
P1	Audit and Accountability	AU-4	Audit Storage Capacity	Ken	
P1	Audit and Accountability	AU-5	Response to Audit Processing Failures	Ken	
P1	Audit and Accountability	AU-8	Time Stamps	Ken	
P1	Audit and Accountability	AU-9	Protection of Audit Information	Ken	
P1	Security Assessment and Authorization	CA-1	Security Assessment and Authorization Policies and Procedures	Kevin / Jim	
P1	Security Assessment and Authorization	CA-3	System Interconnections	Kevin / Jim	Needs discussion. Seems impractical with virtualization
P1	Configuration Management	CM-1	Configuration Management Policy and Procedures	Jim / John / Kevin	
P1	Configuration Management	CM-11	User-Installed Software	Jim / John / Kevin	
P1	Configuration Management	CM-2,6	System Hardening Through Baseline Configurations	Jim / John / Kevin	
P1	Configuration Management	CM-7	Least Functionality	Jim / John / Kevin	
P1	Configuration Management	CM-8	Information System Component Inventory	Jim / John / Kevin	
P1	Contingency Planning	CP-1,2	Contingency Plan Update	All	
P1	Contingency Planning	CP-10	Information System Recovery and Reconstitution	All	
P1	Contingency Planning	CP-9	Information System Backup	All	
P1	Identification and Authentication	IA-1	Identification and Authentication Policy and Procedures	Jim / John / Kevin	
P1	Identification and Authentication	IA-2	Identification and Authentication (Organizational Users)	Jim / John / Kevin	
P1	Identification and Authentication	IA-4	Identifier Management	Jim / John / Kevin	
P1	Identification and Authentication	IA-5	Authenticator Management	Jim / John / Kevin	
P1	Identification and Authentication	IA-7	Cryptographic Module Authentication	Jim / John / Kevin	

AC-17

REMOTE ACCESS

Process Owner	Kevin Stillman / John Green
Process Operator	Network Operations / Help Desk
Occurrence	Ongoing
Scope of Impact	Continually occurring in the background
Additional Documentation	
Performance Target	N/A
Technology in Use	Pulse VPN Appliance, Guacamole, Domain Controllers, Microsoft MFA
Technical Summary	Remote access is delivered to remote employees and contractors via a Pulse VPN appliance and Guacamole server remote access. Help Desk installs VPN client software for SUNY-owned devices. Standard User devices access a VPN network segment that has the same access as a standard user network. IT Operations staff access a network segment that can access management interfaces of IT infrastructure. Employees with non-SUNY devices that are allowed to use VPN do not connect directly to a network segment but are only allowed to Remote Desktop to a secure device on the network. Access is controlled via groups in the domain controller and are assigned by the Help Desk.

Section to be completed by reviewers

Control Objective: The organization: ¹

- Documents allowed methods of remote access to systems;
- Establishes usage restrictions and implementation guidance for each allowed remote access method;
- Monitors for unauthorized remote access to systems;
- Authorizes remote access to the system prior to connection; and
- Enforces requirements for remote connections to systems.

Control: Mechanisms exist to define, control and review remote access methods.

Procedure / Control Activity: Systems Security Developer [SP-SYS-001], in conjunction with Security Architect [SP-ARC-002], Systems Security Manager [OV-MGT-001] and Network Operations Specialist [OM-NET-001]:

- (1) Uses industry-recognized practices to develop a defense-in-depth approach to protecting the network and SUNY System Administration's data.
- (2) Uses vendor-recommended settings and industry-recognized secure practices to implement remote access, in accordance with SUNY System Administration policies and standards, as follows:
 - a. Document allowed methods of remote access to the information system;
 - b. Establish usage restrictions and implementation guidance for each allowed remote access method;
 - c. Monitor for unauthorized remote access to information systems;
 - d. Authorize remote access to information systems prior to connection;
 - e. Enforce requirements for remote connections to information systems;
 - f. Use cryptography to protect the confidentiality and integrity of remote access sessions;
 - g. Automatically disconnect remote access sessions after a period of inactivity; and
 - h. Immediately deactivate vendor and business partner remote access when it is no longer needed.

Template language that may be tweaked. Ensure that actual procedures match these controls



The State University
of New York

System Admin's NIST Framework Adoption

- Team will work independently and asynchronously in Microsoft Teams, but meet bi-monthly to stay on track
- Before COVID we were on track for the July 2020 milestone, but there's still time...





Questions?

www.suny.edu

