Evolving Cybersecurity Strategies
NIST Special Publication 800-53, Revision 4

Federal Computer Security Program Manager's Forum

June 12, 2012

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

NIST SP 800-53, Revision 4 Supports

A New Cyber Defense Vision

Build it right – Continuously monitor

Cyber Defense Vision

Core Principles

- Strong, resilient, penetration-resistant information systems supporting core missions / mission processes.
- Ongoing monitoring of the security state of information systems and environments of operation.
- Continuous improvement in security controls.
- Flexibility and agility in cyber security and risk management activities.

Active Cyber Defenses – The Future

- Develop *risk-aware* mission and business processes.
- Develop and implement *enterprise architectures* with embedded information security architectures that support organizational mission/business processes.
- Use information technology *wisely* considering current threat landscape (capabilities, intent, and targeting).
- Develop and implement robust *continuous monitoring* programs.

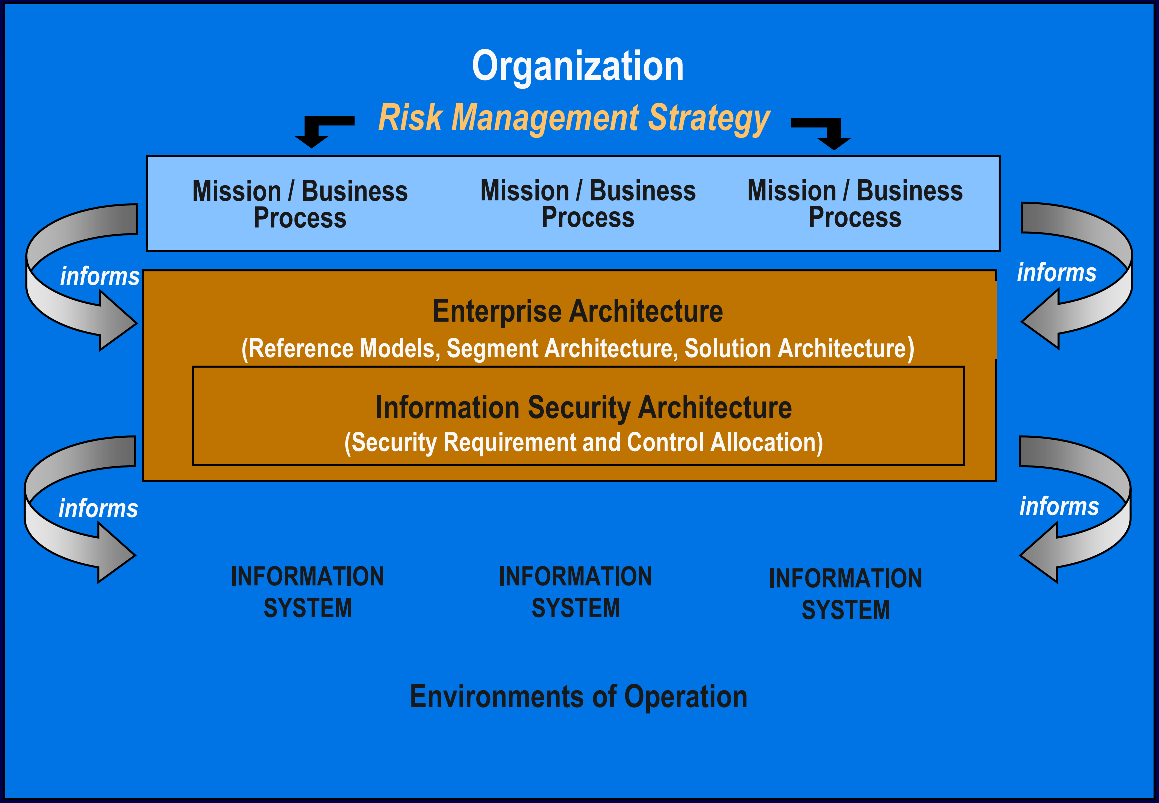
Enterprise Architecture

- Consolidation.
- Optimization.
- Standardization.

And the integration of information security architecture…

- Reduces the size and complexity of IT infrastructures, promotes good cyber security and privacy, and can potentially lower costs (significantly) for organizations.

Architectural and Engineering Approach



Organization

Risk Management Strategy

Mission / Business Process

Mission / Business Process

Mission / Business Process

informs

informs

Enterprise Architecture

(Reference Models, Segment Architecture, Solution Architecture)

Information Security Architecture

(Security Requirement and Control Allocation)

informs

informs

INFORMATION SYSTEM

INFORMATION SYSTEM

INFORMATION SYSTEM

Environments of Operation

Highlights of SP 800-53 Update

Key Milestones

- Received over 1000 comments from national data call in March 2011.
- Interagency team completed adjudication process in October 2011.
- Initial public draft released February 2012.
- Public comment period closed April 2012.
- Final draft targeted for July 2012.
- Final publication targeted for September 2012.

Major Drivers for Update

- Current threat landscape.
- Empirical data obtained from cyber attacks.
- Gaps in coverage in current security control catalog.
- Insufficient attention to security assurance and trustworthiness.
- Need for additional tailoring guidance for specific missions, technologies, and environments of operation.

Gap Areas Addressed

- Insider threat.
- Application security.
- Supply chain risk.
- Security assurance and trustworthy systems.
- Mobile and cloud computing technologies.
- Advanced persistent threat.
- Tailoring guidance and overlays.
- Privacy.

Structural Changes

Security Control Class Designations

Eliminated management, operational, and technical class labels on security control families—

ID	FAMILY	~~CLASS~~
AC	Access Control	~~Technical~~
AT	Awareness and Training	~~Operational~~
AU	Audit and Accountability	~~Technical~~
CA	Security Assessment and Authorization	~~Management~~
CM	Configuration Management	~~Operational~~
CP	Contingency Planning	~~Operational~~
IA	Identification and Authentication	~~Technical~~
IR	Incident Response	~~Operational~~
MA	Maintenance	~~Operational~~
MP	Media Protection	~~Operational~~
PE	Physical and Environmental Protection	~~Operational~~
PL	Planning	~~Management~~
PS	Personnel Security	~~Operational~~
RA	Risk Assessment	~~Management~~
SA	System and Services Acquisition	~~Management~~
SC	System and Communications Protection	~~Technical~~
SI	System and Information Integrity	~~Operational~~
PM	Program Management	~~Management~~

Control Enhancement Naming

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: The information system notifies the user, upon successful interactive logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance: This control is intended to cover both traditional logons to information systems and accesses to systems that occur in other types of architectural configurations (e.g., service oriented architectures). Related controls: AC-7, PL-4.

Control Enhancements:

(1) *PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*
The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) *PREVIOUS LOGON NOTIFICATION | SUCCESSFUL/UNSUCCESSFUL LOGONS*
The information system notifies the user of the number of [*Selection: successful logons/accesses; unsuccessful logon/access attempts; both*] during [*Assignment: organization-defined time period*].

Tables Added to Appendix D

CNTL NO.	**CONTROL NAME** *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**		**A**	x	x	x
PL-2	**System Security Plan**		**A**	x	x	x
PL-2 (1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*	**W**	Incorporated into PL-7.			
PL-2 (2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*	**W**	Incorporated into PL-8.			
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*		**A**		x	x
PL-3	**System Security Plan Update**	**W**	Incorporated into PL-2.			
PL-4	**Rules of Behavior**		**A**	x	x	x
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		**A**		x	x
PL-5	**Privacy Impact Assessment**	**W**	Incorporated into Appendix J, AR-2.			
PL-6	**Security-Related Activity Planning**	**W**	Incorporated into PL-2.			
PL-7	**Security Concept of Operations**					
PL-8	**Security Architecture**					

Assumptions, Baselines, and Tailoring

Clarification of Term *Baseline*

The use of the term *baseline* is intentional. The security controls and control enhancements listed in the initial baselines are *not* a minimum—
but rather a proposed starting point from which controls and controls enhancements may be removed or added based on the tailoring guidance in Section 3.2.

Specialization of security plans is the goal…

Assumptions for 800-53 Rev 4 Baselines

- Assumptions applied when security controls for each baseline were determined.
- Assumptions are a key element in the risk framing step in the NIST SP 800-39 risk management process.
- Assumptions about control selection may be related to:
  - Operational environments;
  - Nature of missions/operations being conducted;
  - Functionality of the information system;
  - Threats facing all three organizational tiers;
  - Information types processed, stored, or transmitted.

Assumptions Applied to Baselines

- Information systems are located in fixed, physical facilities, complexes, or locations.
- User information in systems is (relatively) persistent.
- Information systems are multi-user (either serially or concurrently) in operation.
- Information systems exist in networked environments.
- Information systems are general purpose in nature.
- Organizations have the necessary structure, resources, and infrastructure to implement the security controls.

Assumptions Not Applied to Baselines

- Insider threats exist within organizations.
- Classified information is processed, stored, or transmitted.
- Advanced persistent threats exist within organizations.
- Information requires specialized protection based on federal legislation, Executive Orders, directives, regulations, or policies.
- Information systems communicate or interconnect with systems in different policy domains.

Expanded Tailoring Guidance

(1 of 2)

- Identifying and designating common controls in initial security control baselines.
- Applying scoping considerations to the remaining baseline security controls.
- Selecting compensating security controls, if needed.
- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements.

Expanded Tailoring Guidance

(2 of 2)

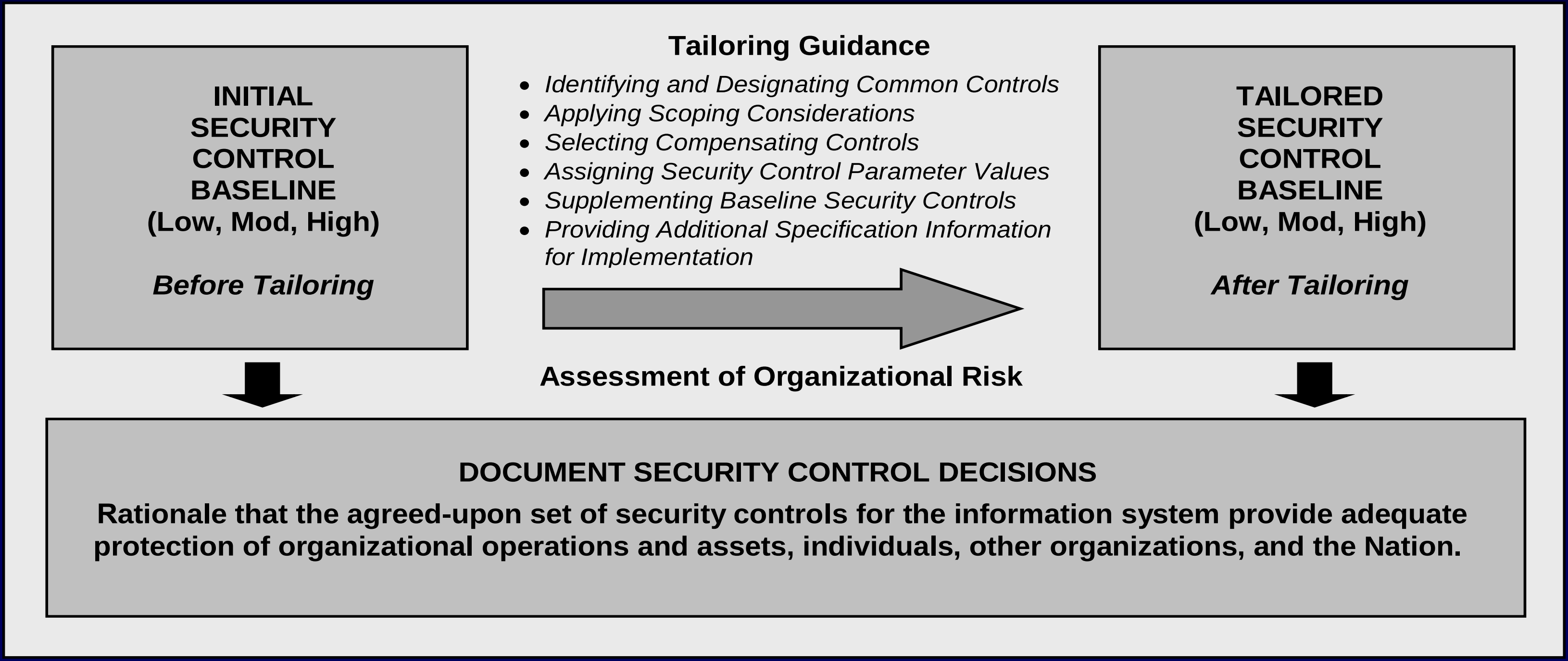
- Supplementing baselines with additional security controls and control enhancements, if needed.

- Providing additional specification information for control implementation.

Supplementing the Baseline

- Inputs may include risk assessment during the security control selection process and/or regulations, policies, etc.
- Example of supplementation for a specific threat—
  - ADVANCED PERSISTENT THREAT
    Security control baselines do not assume that the current threat environment is one where adversaries have achieved a significant foothold and presence within organizations and organizational information systems; that is, organizations are dealing with an advanced persistent threat. Adversaries continue to attack organizational information systems and the information technology infrastructure and are successful in some aspects of such attacks. To more fully address the APT, concepts such as insider threat protection (CM-5 (4)), diversity/heterogeneity (SC-27 and SC-29), deception (SC-26 and SC-30), non-persistence (SC-25 and SC-34), and segmentation (SC-7(13)) can be considered.

Tailoring the Baseline



INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)

Before Tailoring

Tailoring Guidance

- *Identifying and Designating Common Controls*
- *Applying Scoping Considerations*
- *Selecting Compensating Controls*
- *Assigning Security Control Parameter Values*
- *Supplementing Baseline Security Controls*
- *Providing Additional Specification Information for Implementation*

Assessment of Organizational Risk

TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)

After Tailoring

DOCUMENT SECURITY CONTROL DECISIONS

Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

Document risk management decisions made during the tailoring process to provide information necessary for authorizing officials to make risk-based authorization decisions.

Overlays

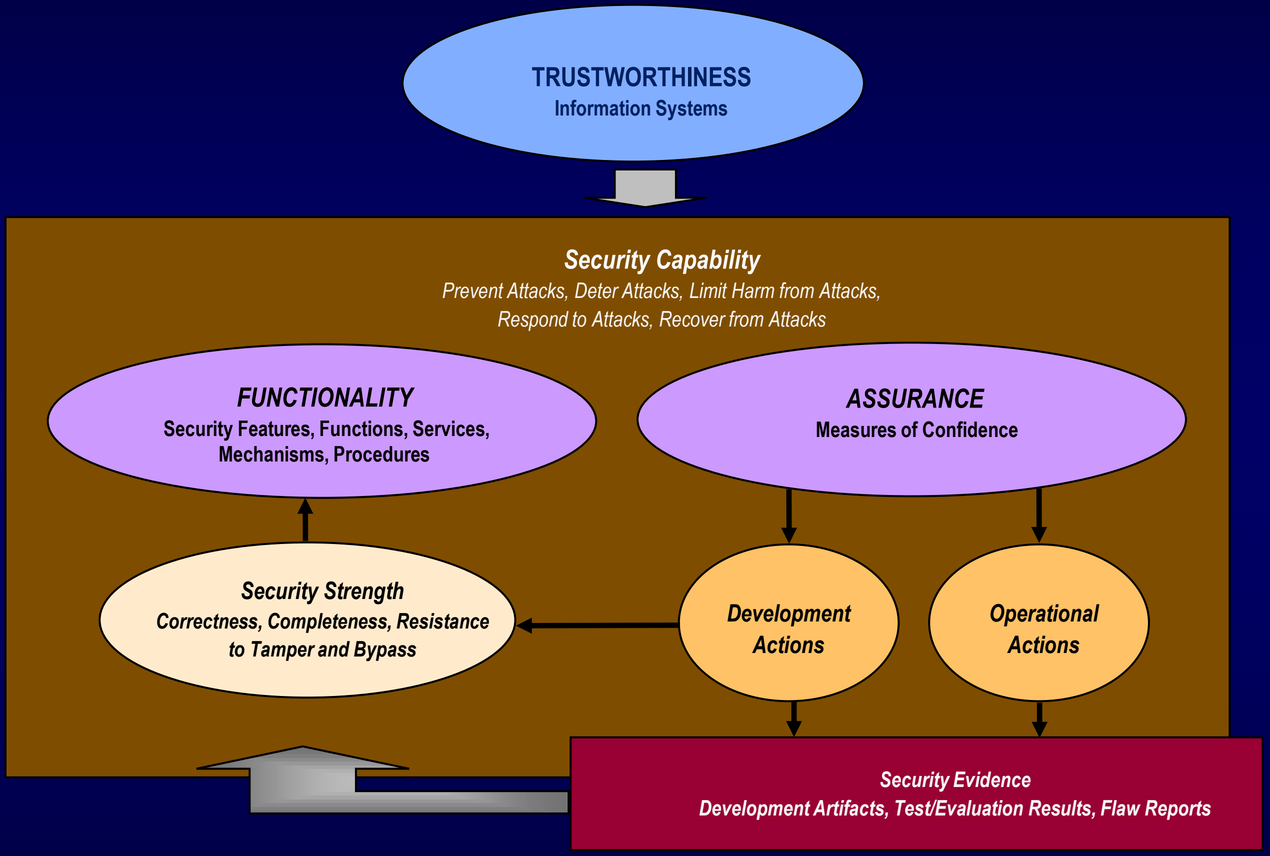
Overlays complement initial security control baselines—

- Provide the opportunity to add or eliminate controls.
- Provide security control applicability and interpretations.
- Establish community-wide parameter values for assignment and/or selection statements in security controls and control enhancements.
- Extend the supplemental guidance for security controls, where necessary.

Types of Overlays

- Communities of interest (e.g., healthcare, intelligence, financial, law enforcement).
- Information technologies/computing paradigms (e.g., cloud/mobile, PKI, Smart Grid).
- Industry sectors (e.g., nuclear power, transportation).
- Environments of operation (e.g., space, tactical).
- Types of information systems (e.g., industrial/process control systems, weapons systems).
- Types of missions/operations (e.g., counter terrorism, first responders, R&D, test, and evaluation).

Assurance and Trustworthiness



TRUSTWORTHINESS
Information Systems

Security Capability
Prevent Attacks, Deter Attacks, Limit Harm from Attacks, Respond to Attacks, Recover from Attacks

FUNCTIONALITY
Security Features, Functions, Services, Mechanisms, Procedures

ASSURANCE
Measures of Confidence

Security Strength
Correctness, Completeness, Resistance to Tamper and Bypass

Development Actions

Operational Actions

Security Evidence
Development Artifacts, Test/Evaluation Results, Flaw Reports

Enables Understanding of Security Capability

Minimum Assurance – Appendix E

- Appendix E has been completely revised and reworked.
- The *minimum* required assurance is provided by implementation of the appropriate baseline set of controls.
- The *assurance-related* controls for each baseline are provided in tables E-1, E-2, and E-3.
- Additional assurance-related controls are provided in table E-4, i.e., assurance-related controls not in any baseline.

Table E-1 - Minimum Assurance for Low Impact Baseline

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-5, SA-9
IA	IA-1	SC	SC-1, SC-41
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

Strengthening of Specification Language

- Significant changes to security controls and control enhancements in—
- Configuration Management (CM) family.
- System and Services Acquisition (SA) family.
- System and Information Integrity (SI) family.

Applying best practices in software development at all stages in the SDLC.

Privacy – Appendix J
(1 of 2)

- Privacy and security are complementary and mutually reinforcing.
- Appendix J complements security controls in Appendix F.
- Privacy control families are the same as those in the FEA Security and Privacy Profile, v3, September 2010.
- Appendix J is based on:
  - Fair Information Practice Principles from Privacy Act of 1974;
  - E-Government Act of 2002, Section 208; and
  - Privacy-related OMB guidance.

Privacy – Appendix J

(2 of 2)

- Objective of Appendix J is to promote closer cooperation between privacy and security officials.
- Intended for organizational privacy officials (e.g., CPOs) working with:
  - Program managers;
  - Information system developers;
  - Information technology staff; and
  - Information security personnel.
- Apply each control with respect to organization's distinct mission and operational needs based on legal authorities and obligations.

Privacy Control Families

- Authority and Purpose **(AP)**
- Accountability, Audit, and Risk Management **(AR)**
- Data Quality and Integrity **(DI)**
- Data Minimization and Retention **(DM)**
- Individual Participation and Redress **(IP)**
- Security **(SE)**
- Transparency **(TR)**
- Use Limitation **(UL)**

Moving to Continuous Monitoring

Policy Changes

OMB 2011 FISMA Reporting Guidance, *Memorandum-11-33*

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf ***Question #28***

- "28. Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?

  No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate reauthorization process is not necessary………."

- Follow guidance consistent with NIST Special Publication 800-37, Revision 1.

Bottom Line: Rather than enforcing a static, every-three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs.

Continuous Monitoring Strategy

- Determine effectiveness of risk mitigation measures.
- Identify changes to information systems and environments of operation.
- Verify compliance.

Bottom Line: Increase situational awareness to help determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

Focus Areas — 2012 and Beyond

- NIST Special Publication 800-30, Revision 1
- Systems and Security Engineering Guideline
- Update to NIST Special Publication 800-53, Revision 4
- Update to NIST Special Publication 800-53A, Revision 2

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov