NASA Cybersecurity

November 20, 2014

Agenda

- Cyber Challenges
- Agency Overview
  - Vision and mission
  - Infrastructure
  - Internal and External Assessments
- Protecting NASA Infrastructure
- Moving Forward

The Not So Friendly Cyber World…

Cybercrime and Espionage costs $445 Billon annually
According to National Security Report…

Chinese Hackers Hit OPM Networks
– New York Times

Commerce IG identifies cybErsecurity risks with NOAA satellite systems
- fedscoop

The U.S. Postal Service the victim of "a cyber-security intrusion"
- FEDSCOOP

Hackers Hit Department of State Email Servers
– Reuters

Public Disclosure of Hacks

We are operating in a contested environment.

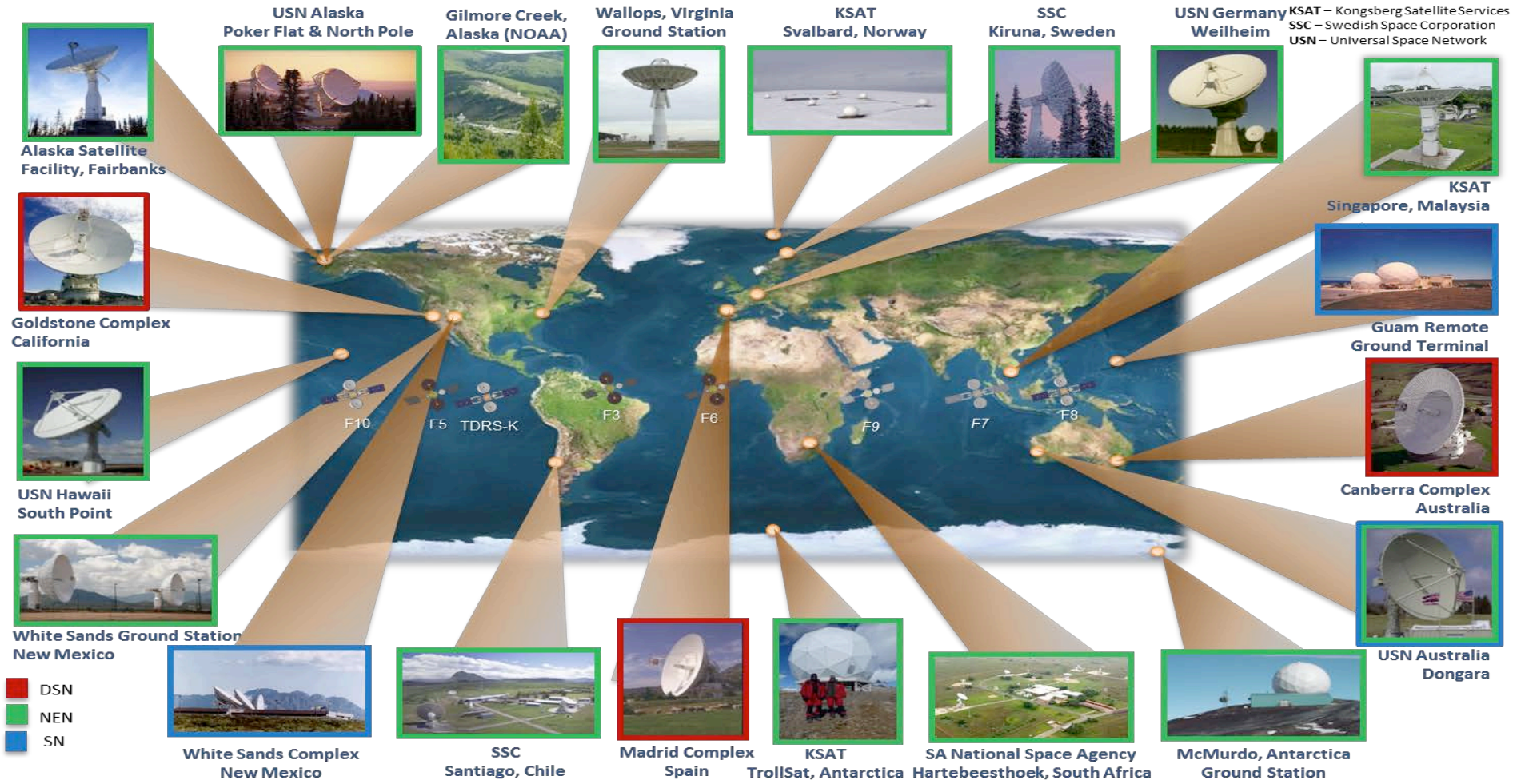
NASA Cyber Operations: A Typical Week

Malicious incidents against NASA systems	**29,000**
Suspicious e-mails	**17,500**
Unique incidents against NASA websites	**250**
Unique high threat e-mail incident	**170**
Advanced attacks against NASA websites	**25**
Lost or Stolen Equipment	**9**
Mitigation actions implemented to prevent incidents	**190**

Agenda

- Cyber Challenges
- Agency Overview
  - Vision and mission
  - Infrastructure
  - Internal and External Assessments
- Protecting NASA Infrastructure
- Moving Forward

NASA IT Overview

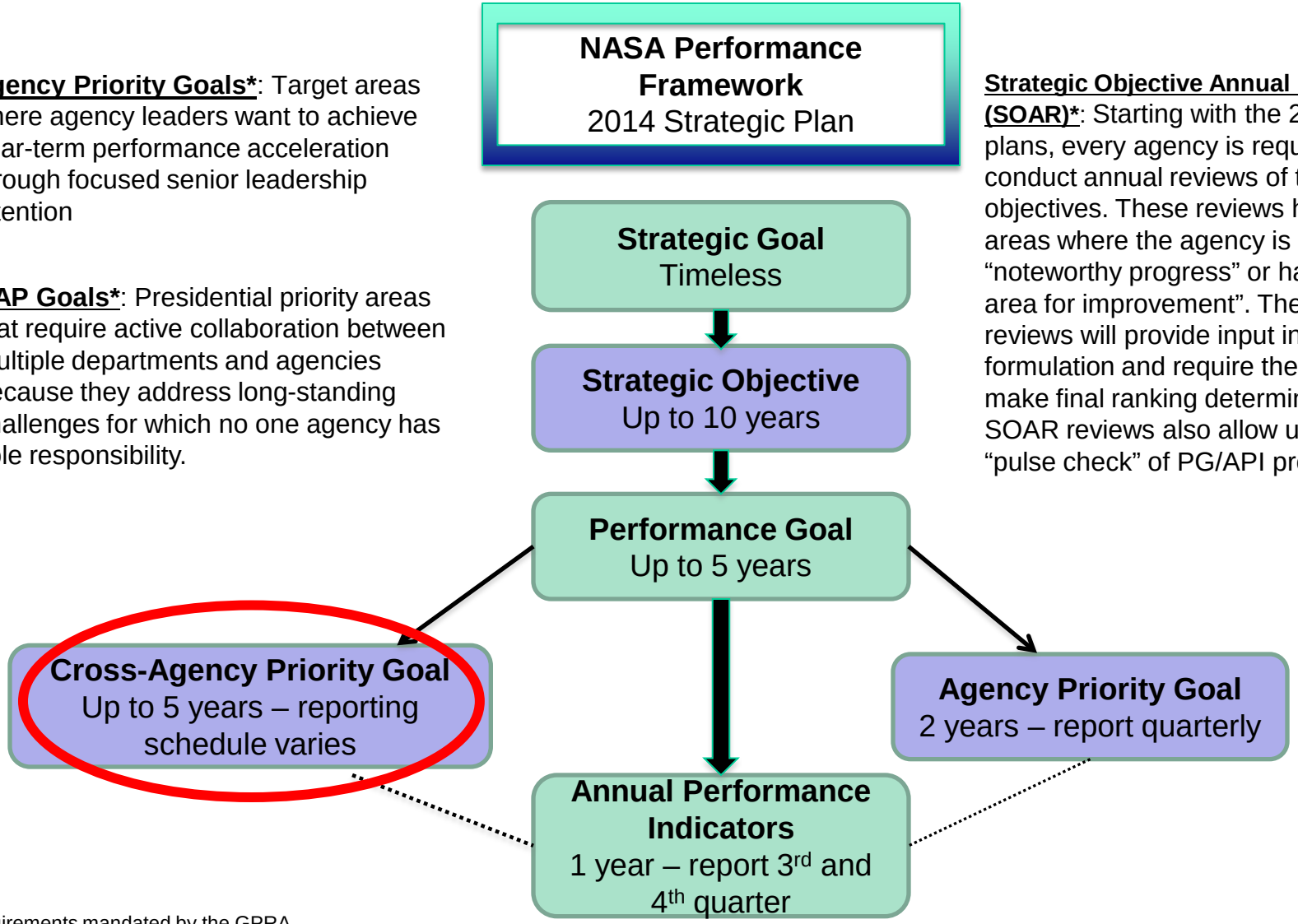


Global Interconnected Infrastructure Supporting our Current and Future Missions and Programs

NASA Strategy-Performance Framework

Agency Priority Goals*: Target areas where agency leaders want to achieve near-term performance acceleration through focused senior leadership attention

CAP Goals*: Presidential priority areas that require active collaboration between multiple departments and agencies because they address long-standing challenges for which no one agency has sole responsibility.



Strategic Objective Annual Review (SOAR)*: Starting with the 2014 strategic plans, every agency is required to conduct annual reviews of their strategic objectives. These reviews highlight those areas where the agency is making "noteworthy progress" or has a "focus area for improvement". These annual reviews will provide input into budget formulation and require the COO/PIO to make final ranking determinations. (Note: SOAR reviews also allow us to conduct a "pulse check" of PG/API progress in Q2.)

*Requirements mandated by the GPRA Modernization Act of 2010 and OMB Circular A-11

Executive Support

- Clear executive support
  - Effective Cyber program providing value to our missions and programs
  - Ready to tell a compelling story
  - Define problems and impacts
  - Demonstrate vision
  - Know what it takes
  - Figure out the price tag
  - Quantify the value

Success Demands a Holistic Solution

Multi-tiered approach that aligns cyber security management to mission assurance and agency performance:

- Better alignment to mission objectives
- Increased readiness, scalability and flexibility
- Global cross-standard application
- Rigorous cycle of risk identification and management
- Future-focus to anticipate emerging challenges

Identify the real risks; **Protect** what matters most; **Sustain** an enterprise program; **Optimize** for mission performance.

Recent Assessments

Organizations across NASA benefits from objective assessments of our information security programs and structures:

- Internal
- External
- OIG
- GAO
- Congressional

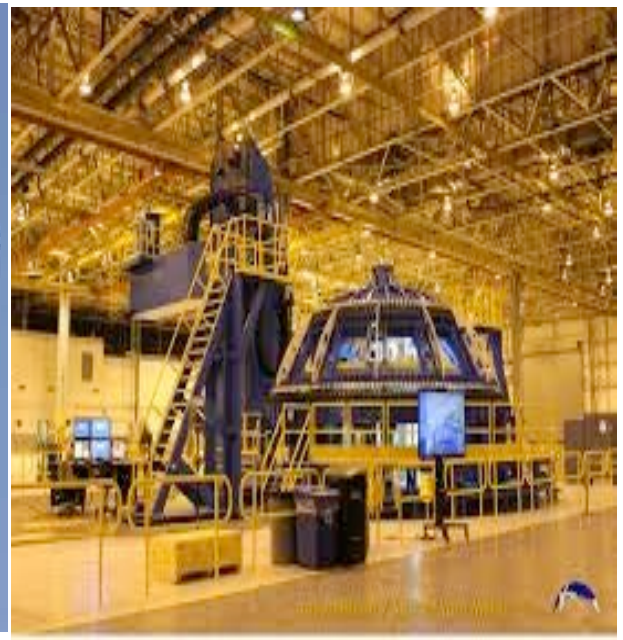
Agenda

- Cyber Challenges
- Agency Overview
  - Vision and mission
  - Infrastructure
  - Internal and External Assessments
- Protecting NASA Infrastructure
- Moving Forward

The Impetus for Mission Protection / Assurance

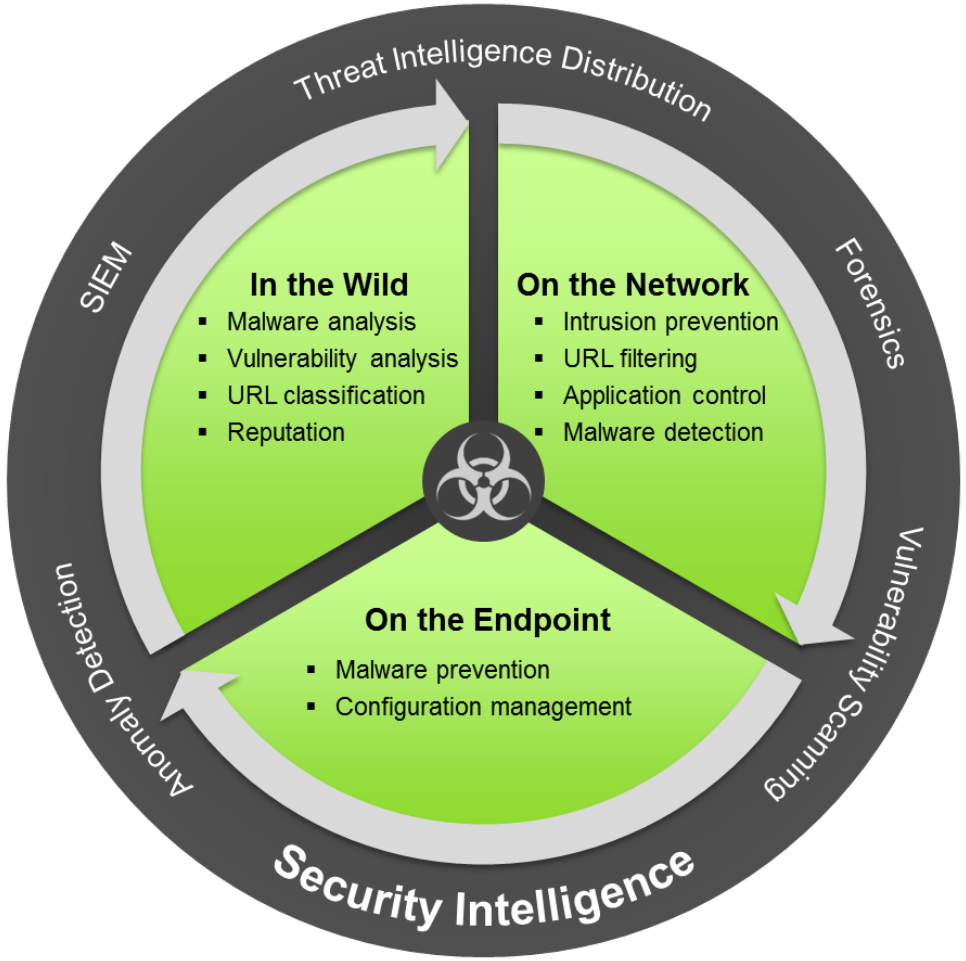
National Capabilities \ Global Interest

- Developed with industry
- Developed using COTs
- Global procurement
- Global Partnerships



Securing NASAs Infrastructure

Advanced Threat Protection



1. Acknowledge that we operate in a contested environment.
2. Threat actors exist as abundantly within as they do outside our boundaries
   - Partnerships, cloud, mobile devices are redefining the enterprise
3. Prioritize vulnerability management to address the most critical enterprise vulnerabilities first!
4. Provide frequent and tailored training.

Cybersecurity: Delivering intelligence, integration and expertise across a comprehensive framework

Intelligence

Integration

Expertise

Prioritize vulnerability management to address the most critical enterprise vulnerabilities first!

NASA Enterprise Security framework

IT Service Security

End Users
- Security Asset Management (SW/HW Inventory, MDM)
- Vulnerability & Patch Management
- Event Management & Application Whitelisting Services

Host
- Virtualization Security
- Cloud Security
- Host based IDS/IPS
- Malware Defenses

Security Operations
- Threat Management
- Log Management
- Security Incident Management
- Forensic Analysis
- Penetration Testing
- Enterprise Cyber Situational Awareness
- Event Monitoring/IDS/IPS
- Security-focused Configuration Management
- Dashboard System

Data & Application Security

Data Security
- Data Classification
- Data Loss Detection & Prevention (Network & Host)
- DAR
- Data in transit encryption

Application Security
- SDLC
- Secure Coding
- Application Scanning
- Application Gateway
- Software Assurance

Infrastructure Security

Network + Communication
- Wireless Protection
- Network Perimeter Protection
- Breach protection& Web Content filtering
- DNS Security
- Secure Network Infrastructure
- Email Security

Server & Application
- Internet Facing Servers Security
- Data warehouse Security

Access Control
- ICAM – Access/Identify Management
- PIV credentials across NASA
- Mobile Device Solution
- FIPS 201-2 (4 Certs on a Card)
- EPACS Upgrade/ Reader Replacement
- Perimeter Access – Center & Agency

Security Policy Framework
- Governance
- Policy
- Strategy
- Roles & Responsibilities
- Metrics & Performance Management
- Risk Management
- Legal & Regulatory
- Education & Awareness

NASA Cyber Security Program

Threat Management

- NASA SOC
- NASA CI
- NASA OIG
- DHS US CERT
- FBI InfraGard
- FFRDCs
- Private Corporations
- Open Source
- Awareness and Outreach
- Penetration Testing
- AVAR
- Threat Analysis

Prevention

- DNS Security
- Patch Management
- Data At Rest (DAR) Encryption
- Account Management and Control
- Network firewalls
- Network Access Control
- Application security
- Configuration Management
- Application whitelisting
- Proxy System
- Administrative Privileges
- Layered Defense(DMZ)

Monitoring and Detection

- Intrusion Detection
- Log Management
- Security Information and Event Mgmt
- Host based-IDS/IPS
- Antivirus and anti-malware
- Web Application Firewall
- Network based Anti-phishing
- Auditing & Forensic Analysis
- WASP
- IPS
- Dashboard System
- Full packet capture
- Host Based Firewall

Containment / Eradication

- Incident Response
- DNS sink hole
- IP sink hole
- Elevated Privilege Management
- Networks Forensics & Visibility
- Network zones

Information Assurance

- Policy
- Requirements
- Guidelines
- Security Plans
- Full Disk Encryption
- Contingency Planning
- SBU/Privacy Program
- CUI Implementation Program
- Data Classification and Protection
- DHCP
- Email Encryption
- Cloud Security
- Mobility Security
- Virtualization

Advance Cyber Defense Tools and Techniques

- Malware Analysis
- Privacy/CUI Assessment Tool
- Security-related Behavior Management
- Network Anomaly Detection
- Data Analytics
- Application Anomaly Detection

Legend
Green: On Going
Yellow: MSC FY14-18
Orange: CDM FY15-16
Red: FY17-18

Enterprise Architecture – Security Capabilities

Capability		Sub-Capability		2014	2015	2016	2017	2018	2019
Continuously Secure and Monitor	Protect Network Perimeter	Provide Network Based Intrusion Detection and Prevention	Perimeter Firewall						
			Application Firewall						
			Network Based Intrusion Detection System (NIDS)						
			Network Based Intrusion Prevention System (NIPS)						
			Wireless Intrusion Detection System						
			Wireless Intrusion Prevention System						
			DNS Sinkhole Security Capability						
			IP Sinkhole Security Capability						
			Network Access Control (NAC)						
			Mobile Device Management (MDM)						
			Automated Behavioral Analysis (AuBA) Pilot						
			Breach Detection (malware)						
			Network Behavior-Based Anomaly Detection						
		Provide Content Monitoring, Inspection, and Filtering	Reverse Proxy						
			Web Content Filtering/Monitoring						
			TIC Sensors DHS Component						
		Provide Web Application Security	Provide Web Application Security						
		Provide Email Security	Provide Email Security						
		Network Security Architecture	Provide Zoned Base Architecture						
		Provide Remote Access Security	Provide Enterprise Remote Access Security						
		Secure DNS	DNSSEC						
	Protect Host Based Perimeter	Provide Malware Defenses	Antivirus and Anti-Malware Protection						
			Application Whitelisting						
			Malware Exploitation Prevention (EMET, DEP)						
			Virtualization Security						
		Host Based Intrusion Detection and Prevention	Host Based Firewall						
			Host Based IDS						
			Host Based IPS						
			Provide Enterprise PKI Encryption						
		Data In Transit Encryption - Security Capability	Data In Transit Encryption - Security Capability						
		Prevent Data Loss	Network Data Loss Prevention						
			Host Based DLP						
		Data Backup and Recovery - Security Capability	Data Backup and Recovery - Security Capability						
	Manage Configuration	Security Asset Management	Authorized and Unauthorized Hardware Inventory						
			Authorized and Unauthorized Software Inventory						
		Security-Focused Configuration Management	Security-Focused Configuration Management						
		Vulnerability Management	Vulnerability Management						
		Patch Management	Patch Management						
Security Information and Event Management	Threat Management	Threat Analysis	Threat Analysis						
	Log Management	Log Aggregation	Log Aggregation						
		Monitor and Audit Logs	Monitor and Audit Logs						
		Log Analysis and Correlation	Log Analysis and Correlation						
		Log Storage and Disposal	Log Storage and Disposal						
		Log Security	Log Security						
	Security Incident Management	Security Incident Management	Security Incident Management						
	Forensic Analysis	Forensic Analysis	Forensic Analysis						
	Penetration Testing	Penetration Testing	Penetration Testing						
	Enterprise Cyber Situational Awareness	DASH Board System	DASH Board System						
Risk Management	Categorization of Information Systems	Categorization of Information Systems	Categorization of Information Systems						
	Selection of Security Controls	Selection of Security Controls	Selection of Security Controls						
	Implementation of Security Controls	Implementation of Security Controls	Implementation of SecurityControls						
	Assessment of Security Controls	Assessment of Security Controls	Assessment of Security Controls						
	Authorization of the Information Systems	Authorization of the Information Systems	Authorization of the Information Systems						
	Monitoring Security Controls	Monitoring Security Controls	Monitoring Security Controls						
	Access Control		Systems and Applications						
			Physical Access Controls						

Prioritized Capabilities

Sub-Capability			2014	2015	2016	2017	2018	2019
Protect Network Perimeter	Provide Network Based Intrusion Detection and Prevention	Perimeter Firewall						
		Application Firewall						
		Network Access Control (NAC) - Internal						
		Mobile Device Management (MDM)						
	Provide Content Monitoring, Inspection, and Filtering	Web Content Filtering/Monitoring						
	Provide Web Application Security	Provide Web Application Security - Scan / Monitor						
	Provide Remote Access Security	Provide Enterprise Remote Access Security - VPN						
Protect Host Based Perimeter	Provide Malware Defenses	Antivirus and Anti-Malware Protection						
		Malware Exploitation Prevention (EMET, DEP)						
	Host Based Intrusion Detection and Prevention	Host Based Firewall						
		Host Based IDS						
		Host Based IPS						
Data Protection and Information Security	Prevent Data Loss	Network Data Loss Prevention						
Security Incident Management	Security Incident Management	Security Incident Management						
Forensic Analysis	Forensic Analysis	Forensic Analysis						

CDM
MSC Bundle 1
MSC Bundle 2/3
Comm. Services
Existing

HWAM
SWAM
CSM
VUL

Critical Security Controls

for Effective Cyber Defense

Critical Security Controls		National Security Agency Assessment of the Critical Controls		
Critical Security Control	Critical Security Control Description	Attack Mitigation	NASA Technical Maturity	Responsible Party
1 Inventory of Authorized and Unauthorized Devices	**Reduce the ability of attackers to find and exploit unauthorized and unprotected systems:** Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.		Medium	Enterprise (EN) Mission Directorates (MD)
2 Inventory of Authorized and Unauthorized Secure Configurations for Hardware & Software on laptops, Workstations, and Servers	**Identify vulnerable or malicious software to mitigate or root out attacks:** Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.		Medium	EN MD
3	**Prevent attackers from exploiting services and settings that allow easy access through networks and browsers:** Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.		Medium	EN MD
4 Continuous Vulnerability Assessment and Remediation	**Proactively identify and repair software vulnerabilities reported by security researchers or vendors:** Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.		Medium	EN MD Centers (CN)
5 Malware Defenses	**Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading:** Use automated anti-virus and anti-spyware software to regularly monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Avoid network devices from using auto-run programs to access removable media.		Medium	EN MD CN

Critical Security Controls

for Effective Cyber Defense

Critical Security Controls		National Security Agency Assessment of the Critical Controls		
Critical Security Control	Critical Security Control Description	Attack Mitigation	NASA Technical Maturity	Responsible Party
6 Application Software Security	**Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).		Medium	EN MD CN
7 Controlled use of Administrative Privileges	**Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack:** (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.		Medium	EN MD CN
8 Boundary Defense	**Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines:** Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (“extranets”).		Medium	EN MD
9 Data Loss Prevention	**Stop unauthorized transfer of sensitive data through network attacks and physical theft:** Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.		Medium	EN MD
10 Penetration Tests and Red Team Exercises	**Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.		High	EN MD CN

Agenda

- Cyber Challenges
- Agency Overview
  - Vision and mission
  - Infrastructure
  - Internal and External Assessments
- Protecting NASA Infrastructure
- Moving Forward

Training / Awareness/ Assessments

- Yearly IT Training
- Phishing Exercises
- Role Based Training
- Secure Code Training
- Focused Assessments

NASA must be prepared to combat against, manage and mitigate cyber attacks that can occur anytime, anywhere.

Cyber hygiene begins and ends with each of and every employee.

Key Takeaway

Success Demands a Holistic Solution

Security is not one technology, it is a combination of People Processes and Technology forming an overall solution to protect our information and IT systems.

We need a multi-tiered approach that aligns cyber security management to mission assurance and agency performance

NASA CIO

Office of the
Chief Information Officer