



NASA Cybersecurity Program

NASA Advisory Council Update

Office of the Chief Information Officer

10 November
2015

NASA OCIO
Information Technology Security
Division

www.nasa.gov





Cybersecurity Program Overview

NIST Cybersecurity Function	Description	NASA's Cyber Programs	Total Budget
Identify	Develop organizational understanding to manage cyber risk to systems, assets, data, and capabilities	<i>See Appendix</i>	\$8,384,247
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services	<i>See Appendix</i>	\$13,004,531
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	<i>See Appendix</i>	\$12,593,045
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	<i>See Appendix</i>	\$3,052,360
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cyber event	<i>See Appendix</i>	\$4,440,000



Primary Compliance Drivers

Federal mandates and compliance metrics from:

- U.S. Congress
 - » Federal Information Management Act (FISMA) of 2002 as amended by the Federal Information Modernization Act of 2014
 - » NASA Authorization Act of 2010, Section 1207
 - » Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2016
- Office of Management and Budget (OMB)
 - » “Cybersecurity Sprint” – Enhancing and Strengthening the Federal Government’s Cybersecurity
 - » M-16-03 – FY15-16 Guidance on Federal Information Security & Privacy Management Requirements
 - » M-16-04 – Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government



Primary Compliance Drivers (cont.)

Federal mandates and compliance metrics from:

- Department of Homeland Security (DHS)
 - » BOD-15-01 – Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems
- President's Management Council (PMC)
 - » PMC Agency Cybersecurity Quarterly Assessments
- National Institute for Standards and Technology (NIST)
 - » NIST 800 Series Publications
 - » NIST Cybersecurity Framework
- Cross-Agency Priority (CAP) Goal
 - » FY15 Cybersecurity Priorities



Developing Cybersecurity Program Performance Metrics

- NASA OCIO has engaged cybersecurity program management experts to develop metrics-driven performance measures for NASA's IT Security program
- OCIO is working to finalize the consulting engagement scope and deliverables
- Results will be used to implement live performance dashboards for all levels of Agency & Center IT management



DHS Cyber Hygiene Report

DHS Cyber Hygiene Report provides weekly vulnerability scan results of public-facing IP addresses across NASA

- Averages <1 critical vulnerability per month due to aggressive remediation policies
- Mitigated ~450 public-facing vulnerabilities, a 30% reduction, in the past 6 months (9/2015 – 3/2016)
- Implemented a NASA Cyber Hygiene Dashboard to empower Center Leadership and IR teams

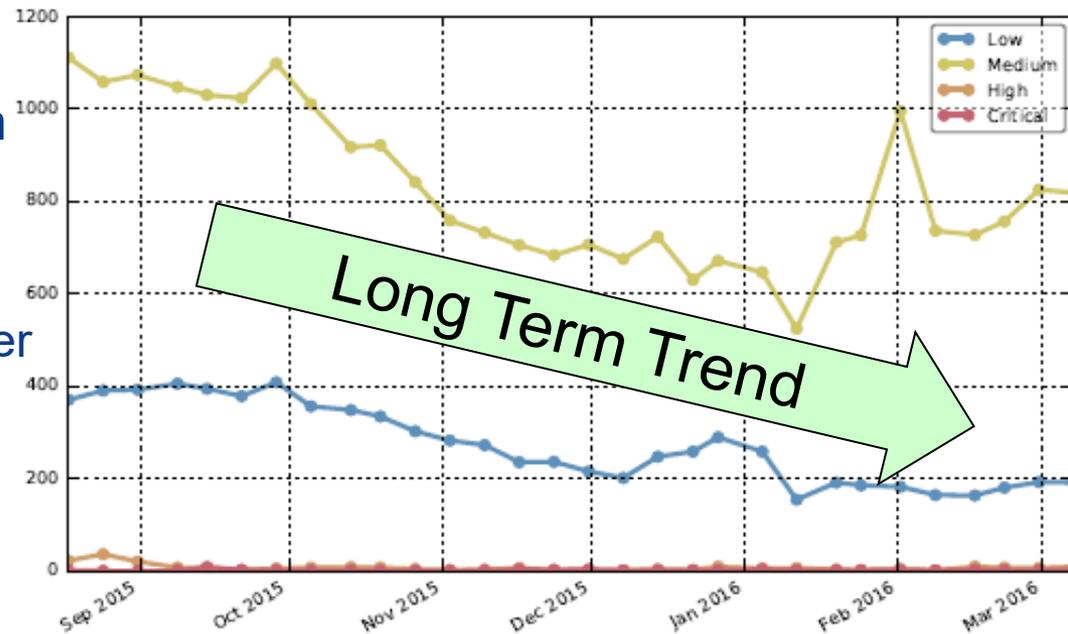


Figure 11: Trending of Total Vulnerabilities by Type

	Current Report	Previous Report	% Change
Hosts	1,349	1,252	7.0%
Vulnerable Hosts	398	396	0.0%
Distinct Operating Systems	187	183	2.0%
Distinct Vulnerabilities Identified	73	75	-3.0%

Table 5: Comparison with Previous Report



Q1FY16 PMC Cyber Assessment

Function	Framework-Based Outcomes	Level-1	Level-2	Level-3
Identify (Level-0)	<ul style="list-style-type: none"> Assets (equipment/software/personnel) and interconnections are all Known/Managed ✓ Vulnerabilities and Risks are Known/Managed ✓ Roles and Responsibilities are clearly outlined ✓ Leveraging FedRAM P-approved services throughout all components/bureaus 	<ul style="list-style-type: none"> CAP Goal: Hardware Asset Mgmt. ≥ 80% CAP Goal: Software Asset Mgmt. ≥ 80% ✓ Policy empowering incident commanders to direct and manage incidents, in place ✓ Review of key contracts with Sensitive Information is in progress 	<ul style="list-style-type: none"> CAP Goal: Hardware Asset Mgmt. ≥ 95% CAP Goal: Software Asset Mgmt. ≥ 95% ✓ Using FedRAM P-approved services Review of key contracts with Sensitive Information is completed ✓ High Value Assets (HVA) identified 	<ul style="list-style-type: none"> CAP Goal: Hardware Asset Mgmt. = 100% CAP Goal: Software Asset Mgmt. = 100% ✓ All contracts handling Sensitive Information contain clauses on protection/detection/reporting of information¹
Protect (Level-0)	<ul style="list-style-type: none"> ✓ All access requires strong authentication • Patch levels are current ✓ Test phishing attempts are caught 	<ul style="list-style-type: none"> ✓ CAP Goal: Vulnerability Mgmt. ≥ 80% • CAP Goal: Secure Config. Mgmt. ≥ 80% ✓ CAP Goal: TIC Consolidation ≥ 80% ✓ CAP Goal: PIV Logical Access ≥ Agency Self-defined Targets (Unprivileged) ✓ CAP Goal: PIV Logical Access ≥ Agency Self-defined Targets (Privileged) ✓ Insider Threat Program in progress 	<ul style="list-style-type: none"> • CAP Goal: Vulnerability Mgmt. ≥ 95% • CAP Goal: Secure Config. Mgmt. ≥ 95% ✓ CAP Goal: TIC Consolidation ≥ 95% • CAP Goal: PIV Logical Access (Unpriv) ≥ 85% ✓ CAP Goal: PIV Logical Access (Priv) = 100% ✓ Insider Threat Program, in place ✓ Initial HVA protection reviews completed ✓ Privileged User count achieved target 	<ul style="list-style-type: none"> • CAP Goal: Vulnerability Mgmt. = 100% • CAP Goal: Secure Config. Mgmt. = 100% • CAP Goal: TIC Consolidation = 100% ✓ Privileged users utilize the same card for privileged and unprivileged accounts
Detect (Level-0)	<ul style="list-style-type: none"> Assets (equipment/software/personnel) and interconnections are actively monitored (e.g., CDM) • Test exfiltration attempts are caught ✓ Attempts to access large volumes of data are detected and investigated ✓ All anomalies reported to SOC and US-CERT 	<ul style="list-style-type: none"> • CAP Goal: Anti-phishing & Malware Defense: 1 of 3 indicators ≥ 90% ✓ Agency ISCM/CDM Program implementation started • Completed implementation of Agency ISCM or D/A Dashboard (CDM Program) ✓ DHS Einstein Program MOA/MOU, per OMB M-15-01, in progress 	<ul style="list-style-type: none"> • CAP Goal: Anti-phishing & Malware Defense: All key indicators ≥ 90% • Agency ISCM/CDM Program Coverage ≥ 95% • Agency assets reported to the Federal CDM Dashboard ≥ 66% ✓ DHS Einstein Program MOA/MOU, per OMB M-15-01, signed ✓ Indicator of Compromise (IOC) scans started within 24 hours of DHS issuance 	<ul style="list-style-type: none"> • CAP Goal: Anti-phishing & Malware Defense: All key indicators = 100% • Agency ISCM/CDM Program Coverage = 100% • Percent of agency assets reported to the Federal CDM Dashboard ≥ 80%
Respond (Level-1)	<ul style="list-style-type: none"> ✓ Roles and Responsibilities are verified in incident response testing • Worst-case Incident Response Plan tested, updated within 30 days of test results ✓ Successful incidents/attacks < 5% or in the top 5 agencies² ✓ Established partnerships for surge resources/special capabilities (contracts/MOAs/MOUs) 	<ul style="list-style-type: none"> ✓ Incident Response Plan developed, tested at least once annually ✓ Ability to measure rate of successful incidents and attacks vs. all incidents² ✓ Participating in C-CAR protocol 	<ul style="list-style-type: none"> ✓ Trending of percentage of successful incidents and attacks is decreasing year-over-year² • Incident Response Plan developed, and tested twice annually ✓ No Active Critical Vulnerabilities > 30 days 	<ul style="list-style-type: none"> • Incident Response Plan developed, and no more than 180 days old ✓ All contracts handling Sensitive Information contain clauses on protection/detection/reporting of information¹
Recover (Level-2)	<ul style="list-style-type: none"> ✓ Business Continuity Plans developed and fully tested for all levels of incidents ✓ Disaster Recovery Plans cover cyber incidents as well as physical loss 	<ul style="list-style-type: none"> ✓ Recovery Plan developed, but not tested regularly ✓ Policy for public/internal notifications conducted within 30 days of detection/discovery, in place 	<ul style="list-style-type: none"> ✓ Recovery Plan developed, tested annually ✓ Ready to leverage Credit Monitoring BPA ✓ Metrics tracking for public/internal notifications conducted within 30 days of detection/discovery, in place 	<ul style="list-style-type: none"> • Recovery Plan developed, and no more than 1 year old ✓ Credit Repair Contract ready for use ✓ Public/internal notifications within 30 days of detection/discovery = 100%



PMC Assessment - IDENTIFY

Function	Framework-Based Outcomes	Level-1	Level-2	Level-3
Identify (Level-0)	<ul style="list-style-type: none"> ◆ Assets (equipment/software/personnel) and interconnections are all Known/Managed ✓ Vulnerabilities and Risks are Known/Managed ✓ Roles and Responsibilities are clearly outlined ✓ Leveraging FedRAM P-approved services throughout all components/bureaus 	<ul style="list-style-type: none"> ◆ CAP Goal: Hardware Asset Mgmt. ≥ 80% ◆ CAP Goal: Software Asset Mgmt. ≥ 80% ✓ Policy empowering incident commanders to direct and manage incidents, in place ✓ Review of key contracts with Sensitive Information is in progress 	<ul style="list-style-type: none"> ◆ CAP Goal: Hardware Asset Mgmt. ≥ 95% ◆ CAP Goal: Software Asset Mgmt. ≥ 95% ✓ Using FedRAM P-approved services ◆ Review of key contracts with Sensitive Information is completed ✓ High Value Assets (HVA) identified 	<ul style="list-style-type: none"> ◆ CAP Goal: Hardware Asset Mgmt. = 100% ◆ CAP Goal: Software Asset Mgmt. = 100% ✓ All contracts handling Sensitive Information contain clauses on protection/detection/reporting of information¹

- CAP Goal: Hardware Asset Mgmt ≥ 80% (Level 1)
- CAP Goal: Software Asset Management ≥ 80% (Level 1)
- Review of key contracts with Sensitive Information to be completed



PMC Assessment – PROTECT

Function	Framework-Based Outcomes	Level-1	Level-2	Level-3
Protect (Level-0)	<ul style="list-style-type: none"> ✓ All access requires strong authentication • Patch levels are current ✓ Test phishing attempts are caught 	<ul style="list-style-type: none"> ✓ CAP Goal: Vulnerability Mgmt. ≥ 80% ◆ CAP Goal: Secure Config. Mgmt. ≥ 80% ✓ CAP Goal: TIC Consolidation ≥ 80% ✓ CAP Goal: PIV Logical Access ≥ Agency Self-defined Targets (Unprivileged) ✓ CAP Goal: PIV Logical Access ≥ Agency Self-defined Targets (Privileged) ✓ Insider Threat Program in progress 	<ul style="list-style-type: none"> ◆ CAP Goal: Vulnerability Mgmt. ≥ 95% ◆ CAP Goal: Secure Config. Mgmt. ≥ 95% ✓ CAP Goal: TIC Consolidation ≥ 95% ◆ CAP Goal: PIV Logical Access (Unpriv) ≥ 85% ✓ CAP Goal: PIV Logical Access (Priv) = 100% ✓ Insider Threat Program, in place ✓ Initial HVA protection reviews completed ✓ Privileged User count achieved target 	<ul style="list-style-type: none"> ◆ CAP Goal: Vulnerability Mgmt. = 100% ◆ CAP Goal: Secure Config. Mgmt. = 100% ◆ CAP Goal: TIC Consolidation = 100% ✓ Privileged users utilize the same card for privileged and unprivileged accounts

- CAP Goal: Secure Configuration Mgmt >= 80% (Level 1)
- CAP Goal: Vulnerability Management >= 95% (Level 2)
- CAP Goal: PIV Logical Access (Unpriv) >= 85% (Level 1)



PMC Assessment - DETECT

Function	Framework-Based Outcomes	Level-1	Level-2	Level-3
Detect (Level-0)	<ul style="list-style-type: none"> ◆ Assets (equipment/software/personnel) and interconnections are actively monitored (e.g., CDM) ◆ Test exfiltration attempts are caught ✓ Attempts to access large volumes of data are detected and investigated ✓ All anomalies reported to SOC and US-CERT 	<ul style="list-style-type: none"> ◆ CAP Goal: Anti-phishing & Malware Defense: 1 of 3 indicators ≥ 90% ✓ Agency ISCM/CDM Program implementation started • Completed implementation of Agency ISCM or D/A Dashboard (CDM Program) ✓ DHS Einstein Program MOA/MOU, per OMB M-15-01, in progress 	<ul style="list-style-type: none"> ◆ CAP Goal: Anti-phishing & Malware Defense: All key indicators ≥ 90% • Agency ISCM/CDM Program Coverage ≥ 95% • Agency assets reported to the Federal CDM Dashboard ≥ 66% ✓ DHS Einstein Program MOA/MOU, per OMB M-15-01, signed ✓ Indicator of Compromise (IOC) scans started within 24 hours of DHS issuance 	<ul style="list-style-type: none"> ◆ CAP Goal: Anti-phishing & Malware Defense: All key indicators = 100% • Agency ISCM/CDM Program Coverage = 100% • Percent of agency assets reported to the Federal CDM Dashboard ≥ 80%

- CAP Goal: Anti-phishing & Malware Defense: 1 of 3 indicators ≥ 90% (Level 1)
- Completed implementation of Agency ISCM Dashboard (CDM Program) (Level 1)
- Agency assets reported to the Federal CDM Dashboard ≥ 66% (Level 2)



PMC Assessment - RESPOND

Function	Framework-Based Outcomes	Level-1	Level-2	Level-3
Respond (Level-1)	<ul style="list-style-type: none"> ✓ Roles and Responsibilities are verified in incident response testing ◆ Worst-case Incident Response Plan tested, updated within 30 days of test results ✓ Successful incidents/attacks < 5% or in the top 5 agencies² ✓ Established partnerships for surge resources/special capabilities (contracts/MOAs/MOUs) 	<ul style="list-style-type: none"> ✓ Incident Response Plan developed, tested at least once annually ✓ Ability to measure rate of successful incidents and attacks vs. all incidents² ✓ Participating in C-CAR protocol 	<ul style="list-style-type: none"> ✓ Trending of percentage of successful incidents and attacks is decreasing year-over-year² ◆ Incident Response Plan developed, and tested twice annually ✓ No Active Critical Vulnerabilities > 30 days 	<ul style="list-style-type: none"> ◆ Incident Response Plan developed, and no more than 180 days old ✓ All contracts handling Sensitive Information contain clauses on protection/detection/reporting of information¹

- Incident Response Plan developed and tested twice annually



PMC Assessment - RECOVER

Function	Framework-Based Outcomes	Level-1	Level-2	Level-3
Recover (Level-2)	<ul style="list-style-type: none"> ✓ Business Continuity Plans developed and fully tested for all levels of incidents ✓ Disaster Recovery Plans cover cyber incidents as well as physical loss 	<ul style="list-style-type: none"> ✓ Recovery Plan developed, but not tested regularly ✓ Policy for public/internal notifications conducted within 30 days of detection/discovery, in place 	<ul style="list-style-type: none"> ✓ Recovery Plan developed, tested annually ✓ Ready to leverage Credit Monitoring BPA ✓ Metrics tracking for public/internal notifications conducted within 30 days of detection/discovery, in place 	<ul style="list-style-type: none"> ◆ Recovery Plan developed, and no more than 1 year old ✓ Credit Repair Contract ready for use ✓ Public/internal notifications within 30 days of detection/discovery = 100%

- Recovery Plan developed and no more than 1 year old



Cross-agency Priority (CAP) Goal Performance

SECTION 1. AGENCY PROGRESS

NASA Internal Target Projections

CAPABILITIES	CAP Goal Targets	Q3FY15	Q4FY15 Target	Q4FY15 Actual	Q1FY16 Target	Q1FY16 Actual	Q2FY16 Target	Q3FY16 Target	Q4FY16 Target	Q1FY17 Target	Q2FY17 Target	Q3FY17 Target	Q4FY17 Target
Hardware Asset Management	95%	0%	1%	0%	1%	4%	15%	45%	65%	75%	85%	90%	95%
Software Asset Management	95%	0%	0%	2%	45%	10%	90%	92%	100%				
Vulnerability and Weakness Management	95%	84%	85%	91%	90%	91%	95%						
Secure Configuration Management	95%	78%	87%	86%	88%	75%	90%	95%					
Unprivileged Network Users	85%	66%	66%	76%	70%	75%	75%	80%	85%				
Privileged Network Users	85%	55%	55%	100%	60%	100%	60%	65%	70%	75%	80%	85%	100%
Anti-Phishing Defense	90%	8%	35%	8%	55%	8%	80%	90%					
Malware Defense	90%	9%	35%	10%	55%	20%	80%	90%					
Blended Defense	90%	11%	35%	17%	55%	17%	80%	90%					

- FY16 CAP Goals Capabilities are calculated from FISMA metrics
- OCIO projected internal metric targets through Q4 FY17
- In Q1 FY16, most capabilities met their *NASA Internal Target %*
 - » **But**, only Privileged Network Users achieved it's *CAP Goal Target*

NASA is improving its performance in key Federal cybersecurity capabilities...



Key Initiatives & Plans

Target Area	Improvement to NASA Cybersecurity	Expected Completion
1. Hardware Asset Management	<ul style="list-style-type: none"> Implementing a Network Access Control (NAC) solution to provide an asset detection and notification capability Implementing CDM Phase 1 tools which improve hardware asset management ability 	Q3 FY16 – Q3 FY17
2. Software Asset Management	<ul style="list-style-type: none"> Deploying the Microsoft Enhanced Mitigation Experience Toolkit (EMET) to help prevent software vulnerability exploitation CDM Phase 1 tools will include an Application Whitelisting capability which improves software management 	Q3 FY16; Q4 FY16
3. Vulnerability & Weakness Management	<ul style="list-style-type: none"> Deploying NASA RISCs infrastructure to improve IT security and vulnerability management Mitigating public-facing vulnerabilities from DHS scan results 	Q3 FY16



Key Initiatives & Plans (cont.)

Target Area	Improvement to NASA Cybersecurity	Expected Completion
4. Secure Configuration Management	<ul style="list-style-type: none"> • CDM Phase 1 Implementation will significantly improve secure configuration management and compliance • CDM will support standardizing asset configurations and allow NASA to uphold periodic scanning and testing intervals in a federated environment 	Q3 FY16 – Q3 FY17
5. Unprivileged Network Access	<ul style="list-style-type: none"> • NASA surpassed the OMB Cyber Sprint's target of 75% of unprivileged users required to use PIV 	Completed (Q4 FY15)
6. Privileged Network Access	<ul style="list-style-type: none"> • NASA met the OMB Cyber Sprint's target as well as the CAP Goal of 100% of privileged users required to use PIV 	Completed (Q4 FY15)

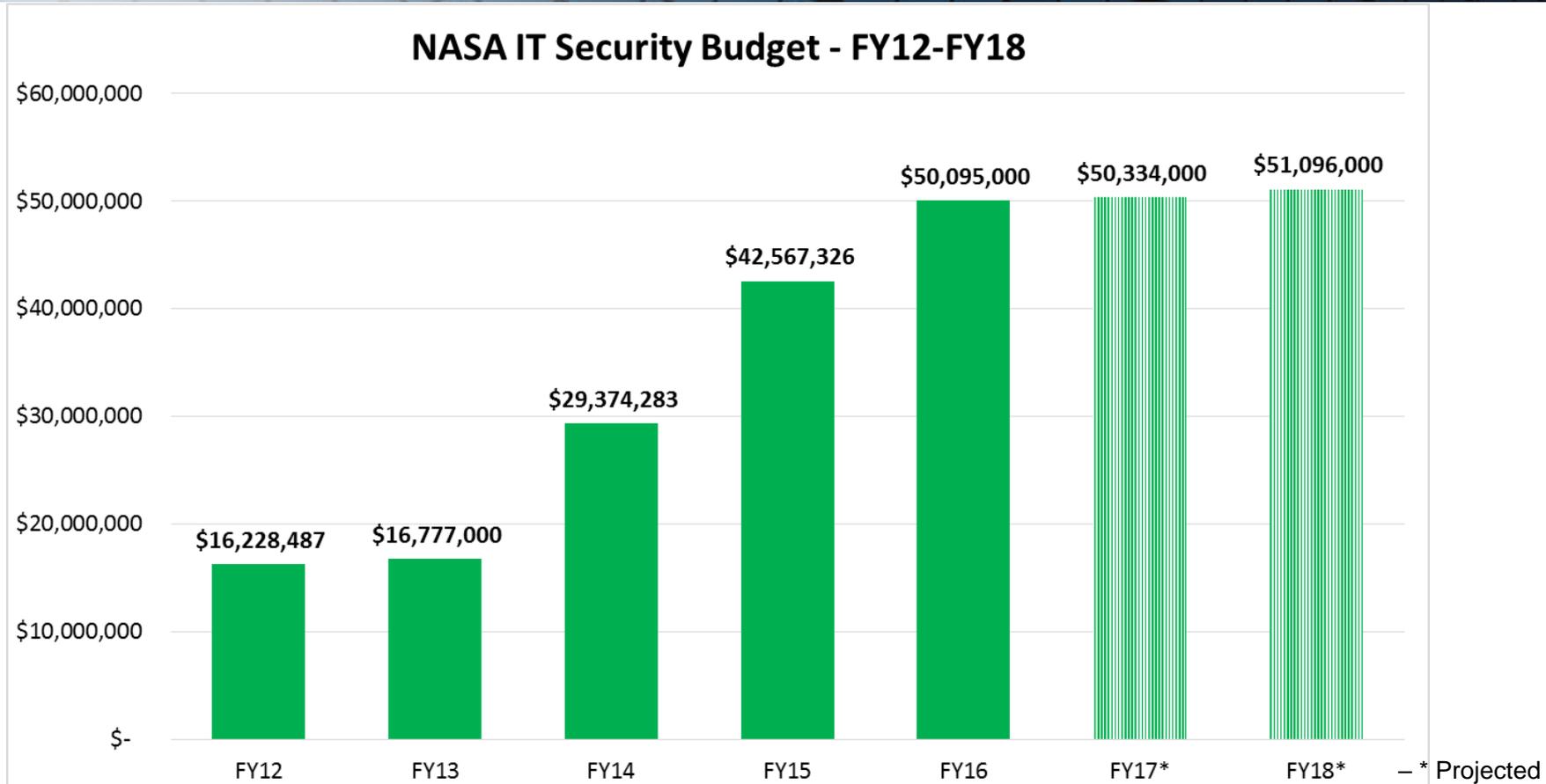


Key Initiatives & Plans (cont.)

Target Area	Improvement to NASA Cybersecurity	Expected Completion
7. Anti-phishing Defense	<ul style="list-style-type: none">• Procured anti-phishing service to train Agency users• Implementing upgrade to email gateway which will significantly reduce phishing emails	Q2 FY16
8. Malware Defense	<ul style="list-style-type: none">• Microsoft EMET improves ability to prevent malware intrusions and exploitations on information systems• Implementing Endpoint Threat Detection & Response (ETDR) tool to detect and investigate suspicious activities• Implementing Symantec Endpoint Protection capability	Q3 FY16
9. Blended Defense	<ul style="list-style-type: none">• Enterprise Border Protection includes Agency-wide solutions for intrusion protection, endpoint protection, web application firewalls (http, https), TLS/SSL inspection, VPN, and web content firewalls• Implementing a Data Loss Prevention (DLP) solution to monitor data exfiltration attempts	Q3 FY16; Q4 FY16



IT Security Budget Over Time



In FY14, NASA significantly increased its IT security budget, enabling OCIO to make critical enhancements to NASA's cyber program and improve its risk posture



Zero-Based Review (ZBR)

- In May 2015, the BSA requested OCIO charter an independent Zero-Based Review of NASA Cybersecurity budget
 - » Analysis of spending to review CDM cost reduction opportunities and other duplicative spending
 - » Scope is limited to OCIO/AMO & CMO funded services, spending by mission funded projects is not in scope
 - » Report completed December 2015
 - » Results will be used in IT Security Service Office planning and budget development



Conclusion: Next Steps

- Implementation of a Risk Management Framework and Cybersecurity program infrastructure is a focus this FY
- CDM implementation is a key strategy to transition Cybersecurity services to the enterprise level
- OCIO implementing live dashboards of performance measures and seek best practices with industry and government partners

Appendix





Cybersecurity Program Overview

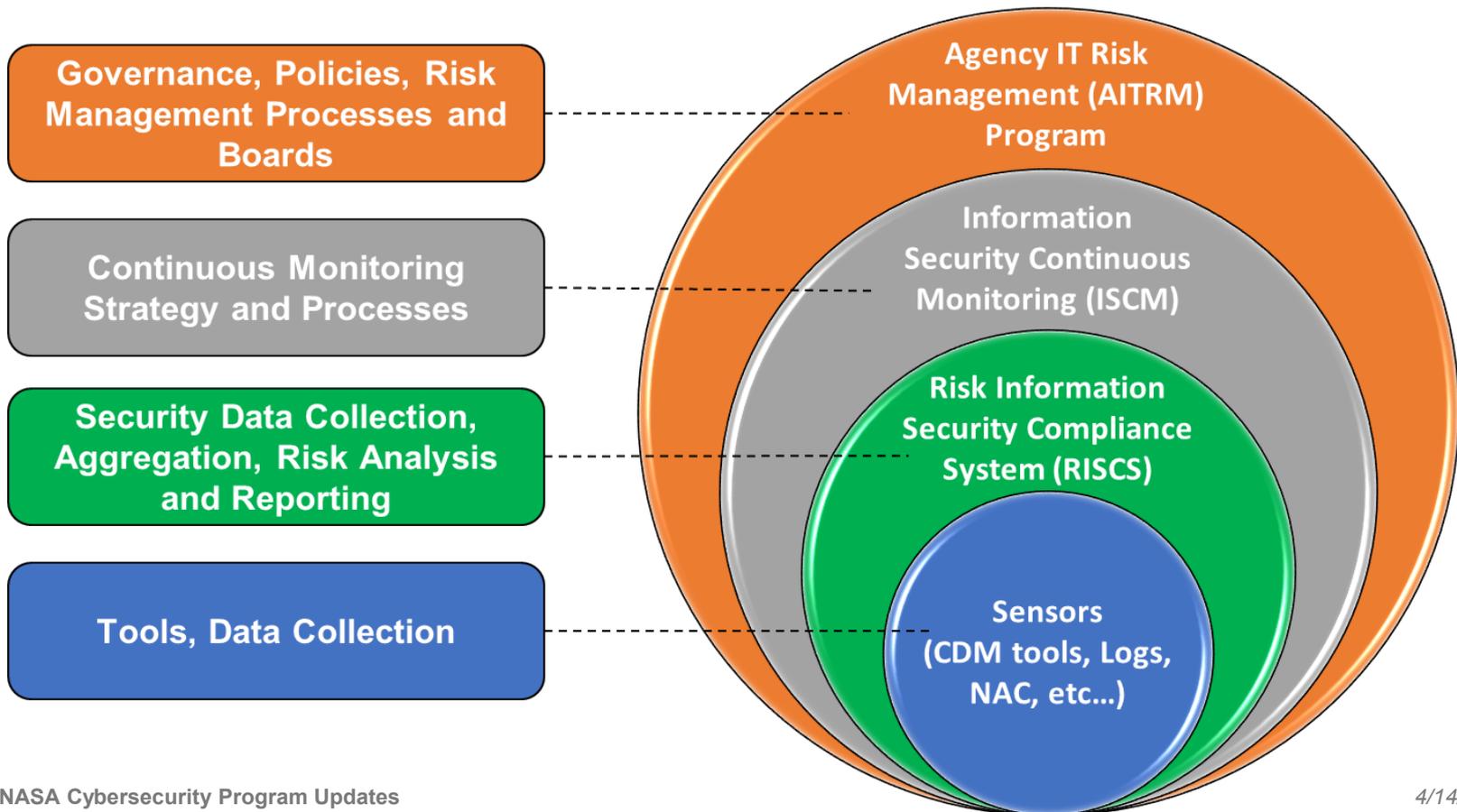
FUNCTION	DESCRIPTION	NASA'S CYBER PROGRAMS			TOTAL EXPENDITURE
 Identify	Develop organizational understanding to manage cyber risk to systems, assets, data, and capabilities.	<ul style="list-style-type: none"> Agency IT Risk Management - Risk Awareness (AITRM - Risk Awareness) Data Classification and CUI Enterprise Security Architecture (ESA) 	<ul style="list-style-type: none"> ITSEC Mgmt Program ITSEC-EDW NASA Security Assessment & Authorization Repository (NSAAR) NOC/SOC Integration 	<ul style="list-style-type: none"> Risk Information Security Compliance System – Asset Info (RISCS – Asset Info) Supply Chain Risk Management 	\$8,384,247
 Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services.	<ul style="list-style-type: none"> Agency IT Risk Management - Processes (AITRM - Processes) Agency Security Configuration Standards (ASCS) *Anti-phishing Tool* Phishing Exercise Application Whitelisting *Cloud Security* 	<ul style="list-style-type: none"> Data at Rest (DAR) *EB Pro* *EIB-NAC* Enhanced Mitigation Experience Toolkit (EMET) *ICAM Enhancement* *IPS* IT Security Awareness & Training Center (ITSATC) 	<ul style="list-style-type: none"> Secure Web Coding Training SOC DNS Sinkhole SOC IP Sinkhole SOC NetMC SOC Ops – Prevention & Mitigation Risk Information Security Compliance System – Fix Actions (RISCS – Fix Actions) Web Application Secure Code Repository 	\$13,004,531
 Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	<ul style="list-style-type: none"> Advanced Analytics Agency Security Update System (ASUS) Agency Vulnerability Assessment & Remediation (AVAR) AuBA Pilot Code Analysis Continuous Diagnostics and Monitoring (CDM) 	<ul style="list-style-type: none"> End User DLP Endpoint Threat Detection and Response (ETDR) Intrusion Detection System (IDS) Network Data Loss Prevention (DLP) Pentest SOC Continuous Monitoring Risk Information Security Compliance System – Scanning (RISCS – Scanning) 	<ul style="list-style-type: none"> SOC Data Loss Prevention (DLP) SOC Ops – Monitoring & Detection SOC Sensors (Breach Detection) WASP Web Inspect Vulnerability Assessment Program (VAP) 	\$12,593,045
 Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	<ul style="list-style-type: none"> Incident Management System (IMS) Modernization 	<ul style="list-style-type: none"> DFAAR 		\$3,052,360
 Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cyber event.	<ul style="list-style-type: none"> SOC Continuity of Operations Plan 	<ul style="list-style-type: none"> SOC Life Cycle Refresh Project 		\$4,440,000

* = ES&I DELIVERED PROJECTS



Risk Management Framework (RMF)

NASA Business Services Assessment (BSA) Team decision for IT Security: “Establish an Agency IT Security risk management framework...”





Continuous Diagnostics & Mitigation (CDM)

CDM enhances NASA's network security through automated control testing and progress tracking.

CDM provides NASA with:

- Improved ability to identify IT security systems and vulnerabilities
- Prioritize actions based on risks
- Sensors to collect IT security data

CDM Phase 1 Implementation will be completed by end of 2016

- Pilot deployment at KSC by end of Q3 FY16





Risk Information Security Compliance System (RISCS)

RISCS – a centralized toolset (COTS), integrates data sources (including CDM) to provide a holistic, risk-based view of our IT systems and operating environment.

OCIO is implementing RISCS in a four phase plan and will enable:

- Assigning risk to the appropriate IT System Security Plan
- Aligning NASA's IT Security controls to the NIST Cybersecurity Framework
- Reporting Agency risk data to the Federal Dashboard

Implementation Timeline

- Phase 1 – Q3 FY16
- Phase 2 – Q1 FY17

RISCS includes modules for:

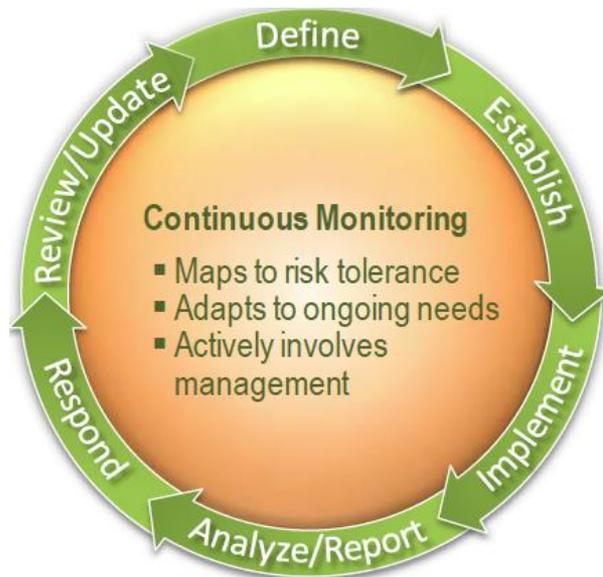




Information Security Continuous Monitoring (ISCM)

ISCM is a risk-based strategy to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

NASA's ISCM Strategy organizes the tools, processes, and information enabled by CDM and RISCs for an effective risk management framework



- In FY15, NASA updated its ISCM Strategy to align with new risk management projects and to reinforce an enterprise solution
- NASA ISCM Strategy is 100% compliant with NIST ISCM and ongoing authorization guidance
- As the Agency IT Risk Management program matures, NASA will revise its ISCM Concept of Operations



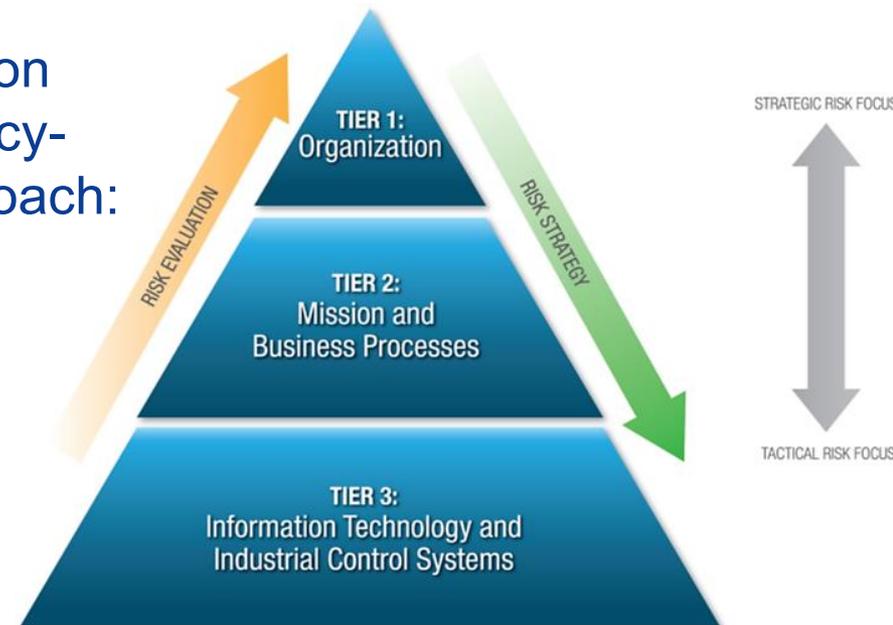
Agency IT Risk Management (AITRM) Program

AITRM integrates technical capabilities, reporting requirements, management processes, and the roles/responsibilities essential to mitigating risk, improving risk posture, and enabling risk-based decision making.

AITRM Program integrates risk information from multiple sources to enable an Agency-level, multi-tiered risk management approach:

- CDM tools
- RISCs modules
- SOC Incident Management System data
- Federal compliance metrics (e.g. FISMA)
- IT Security Training compliance data

AITRM Implementation Plan submitted to BSA Team for approval by April 2016.



NIST Multi-tiered Risk Management Framework