



Overhauling NASA's IT Governance Structure & Ensuring a Safe, Reliable and Secure Agency Network

Office of the Chief Information Officer

Larry Sweet
NASA CIO
July 29, 2014

www.nasa.gov





Leadership Thought

“We are all faced with a series of great opportunities - brilliantly disguised as unsolvable problems.”

John W. Gardner



CIO Vision

The NASA CIO will be responsible for all IT, except ‘highly specialized’ Mission and Program IT

- To provide value-added services as seen by our customers
- To be connected to our many federal initiatives
- To improve IT Security
- To work out inefficiencies and reduce costs in our current programs – “thinking like an Agency”
- To maximize the use of Enterprise and shared services
- To be forward thinking, leveraging new IT advancements where IT benefits NASA and makes NASA better –”shape our future”





IT Challenges

- Increasing Security threats
- Dwindling budgets across the Federal Government
- Retiring workforce
- Vendor management
- Enabling a mobile workforce
- Leveraging Cloud technologies
- Evolving with new technologies – meeting customer expectations





CIO Priorities in FY 2015

- Progressing “Enterprise First” goals
- Increasing Enterprise Communication/Outreach
- Maturing the IT Organization
- Strengthening IT Leadership
- Advancing Portfolio Management in the improvement of IT Spend
- Using Enterprise Architecture to better align Center Initiatives
- Building Trust between OCIO and Center Leaders





NASA IT Culture Today vs. Tomorrow

Present State	Future State
Mission driven-staff does what it takes for the mission	Mission-driven, but will rely on shared resources
Centers enjoy sense of autonomy, lack of confidence in OCIO	Increase confidence and trust by delivering by “Enterprise”
10 Centers run like 10 cities	We will function as “one”
Center mission initiatives drive formulation of budgets; these budgets not always under oversight of HQ	Enterprise has insight into all IT budgets; Budgeting and accountability aligned at OCIO level for all IT spending
Multiple tools and solutions used by more than one center	Highly specialized, mission embedded systems are “owned by programs, but OCIO will influence security & architecture policies
Expertise related to specific missions and programs resides at Centers	Architecture and policies define how expertise is used at different levels of decision making
If Center can prove overriding reason for one off solution, will always win	Vendor Management Office defines how we can be a smart buyer



Organizational Changes

- **Outline a plan for Organizational Change Management**
 - Agency leadership must embrace OCIO reorganization
 - Communicate with employees-not at them, explain the need for change
 - Refine organizational planning and conduct ongoing analyses
 - Set milestones

- **High level outline plans/roadmaps for**
 - Defining decision rights
 - Implementing Centralized Vendor Management Group
 - Implementing Centralized Architecture Governance Group
 - Implementing Functions of Excellence focused on delivering value through services





Functions Of Excellence

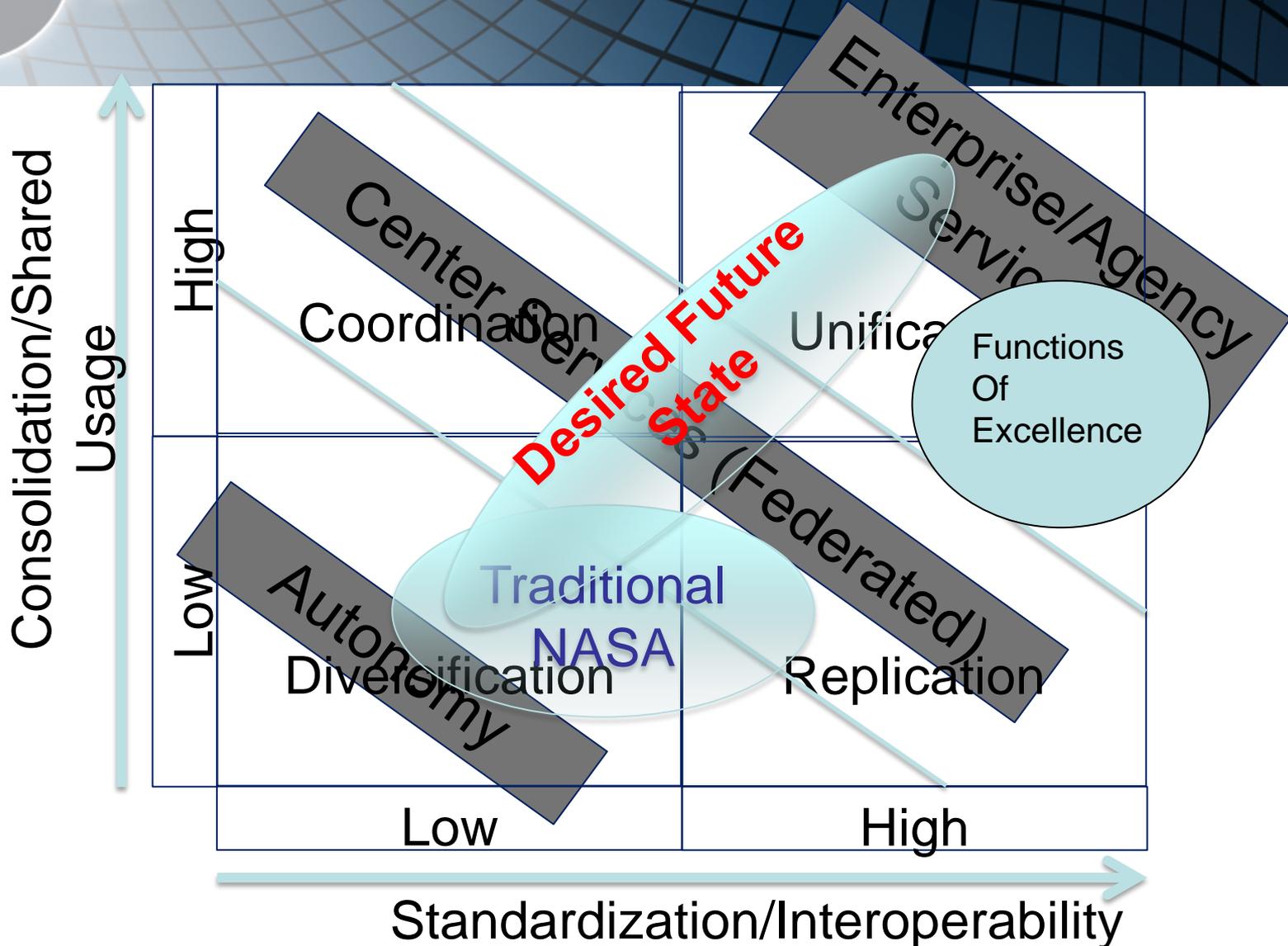
Definition: Services managed/provided by one Center and used by one or more other Centers

Examples: ESD, ESRS, ELMT, SOC, STI, ACES, NICS, NEACC, ETADS, etc.

Opportunities: Help Desk, SharePoint, Maximo, etc.

Questions to address: How do we decide? Is there a standard model? Should there be? What are the barriers?

Desired Future State





Functions of Excellence Summary

- Center inputs can be utilized to prioritize Functions of Excellence activities
- Opportunities for Agency-wide system/service consolidation exist based on Center inputs:
 - SharePoint (internal & external)
 - Data Center Services / Disaster Recovery
 - Asset Management tools
- Commonalities in software utilization between Centers lends itself to Agency-managed software licensing to preclude unnecessary purchases (i.e. Agency APM)



Governance Progress

- OCIO is making progress towards improving the Agency's IT management decision-making
 - This includes the realignment of authority and responsibilities and how we spend Government money
- The OIG's audit made eight recommendations to improve NASA's IT governance structure





NASA IT Governance

- NASA initiated a new IT governance model in 2011 with a three phased approach. Phase 2 approved in 2013 provided better decision making across the Agency
 - Mission Support Council to serve as Agency Decision Body
 - Agency CIO to review and approve all Institutional IT spend and investment based on portfolio reviews
 - Mission Support Council with 6 core members
- Focus on increasing use of Enterprise Services, reducing duplications, improving efficiencies, and ensuring that stakeholder needs are being addressed



Governance Summary

NASA IT Governance

- Three Phased Approach
- Addressing IG Audit Recommendations and Actions
- Draft FITARA legislation

Recent Successes

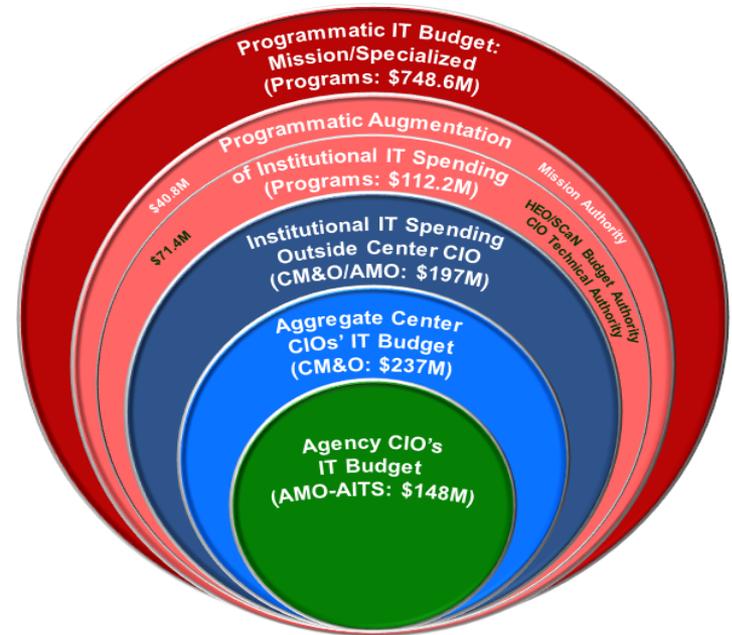
- MSC Phase II approval – CIO visibility and oversight of Center IT spend
- Budget Formulation under Phase II and associated lessons learned for improvement
- Review and update of governing board structure

Looking ahead

- Executing Phase II - institutional
- Defining Phase III – non-highly specialized mission
- End State

*The FY 13 IT budget is enacted

FY13 NASA IT Budget (\$1,442.8M)



Organization	IT Budget (FY13)	Visibility	Involvement of CIO in Governance	Responsibility of CIO for Management	Phase
OCIO (Institutional)	\$148M	Full	Direct Participation	Directly manages	I
Centers (Institutional)	\$434M	Improved since 2011	CIO Delegates to Center CIO for Participation	Directly manages Center CIO, but not Center Resources	II
Programs (Missions)	\$860.759M	Exhibit 300s and SBICs	None	Unclear/Subjective	III



Governance Benefits

- **Improved Agency visibility into IT Investments**
 - seeking out duplications and redundancies
 - help maximize existing capabilities (enterprise services)
- **Ultimate Goal: Optimize the use of IT funds** to ensure the Agency receives the greatest value for its investments





State of NASA Cybersecurity

- NASA continues to identify and mitigate a voluminous number of intrusions that lead to a profound and negative impact on our mission assurance posture.
- NASA is continuing to enhance our resilience by:
 - Collaborating with internal and external partners
 - Integrating services and operations across NASA
 - Improving Risk Management Framework
 - Defining risk thresholds
 - Mitigating or Accepting risks based on mission requirements
 - Defining and implementing consequence of actions





Cybersecurity Challenges

- **Hostile Attacks:** NASA is a key target for persistent malicious attackers
 - There are advanced attacks targeting NASA applications, systems and users
- **Limited Visibility:** The NASA SOC does not have the data, network visibility and causal information to detect and mitigate all incidents across the Agency
 - Robust infrastructure needed to integrate mission and program IT data
- **Mobile Workforce:** NASA's workforce uses devices on and off NASA networks
 - Data Protection and Asset Protection must be improved





NASA Cyber Security Program

Threat Management	Prevention	Monitoring and Detection	Containment / Eradication	Information Assurance	Advance Cyber Defense Tools and Techniques
NASA SOC	DNS Security	Intrusion Detection	Incident Response	Policy	Malware Analysis
NASA CI	Patch Management	Log Management	DNS sink hole	Requirements	Privacy/CUI Assessment Tool
NASA OIG	Data At Rest (DAR) Encryption	Log aggregation	IP sink hole	Guidelines	Security-related Behavior Management
DHS US CERT	Account Management and Control	Security Information and Event Mgmt	Elevated Privilege Management	Security Plans	Network Anomaly Detection
FBI InfraGard	Network firewalls	Host based-IDS/IPS	Networks Forensics & Visibility	Full Disk Encryption	Data Analytics
FFRDCs	Network Access Control	Antivirus and anti-malware	Network zones	Contingency Planning	Application Anomaly Detection
Private Corporations	Application security	Web Application Firewall		SBU/Privacy Program	
Open Source	Configuration Management	Network based Anti-phishing		CUI Implementation Program	
Awareness and Outreach	Application whitelisting	Auditing & Forensic Analysis		Data Classification and Protection	
Penetration Testing	Proxy System	WASP		DHCP	
AVAR	Administrative Privileges	IPS		Email Encryption	
Threat Analysis	Layered Defense(DMZ)	Dashboard System		Cloud Security	
		Full packet capture		Mobility Security	
		Host Based Firewall		Virtualization	

Legend
 Green: On Going
 Yellow: Near Term 6-9 Months)
 Orange: Mid Term 9-14 Months
 Red: Long Term 14-20 Months



Continued Enhancement of NASA Cybersecurity Program

Support Mission Operations

Provide repeatable, sustainable enterprise capabilities in support of NASA's legacy and emerging missions.

- Office of the Chief Information Officer
 - Security Operations Center
 - Network Operations Center
- Office of Protective Services
 - Counter Intelligence
 - Physical Security
- Office of Inspector General
- Mission Directorates

Succeeding in Today's Operations

Develop and vet policies and procedures that can be effectively implemented and monitored

- Provide Strategic Advantage
- Enable Tactical Advantage
- Detect Contain and Mitigate Intrusions and Attacks
- Enhance Cybersecurity Operations

Preparing for the Future

- Enhance acquisition processes to ensure delivery of secure systems and software
- Research, test, and rapidly deploy next generation capabilities to secure NASA's Networks and IT Systems
- Build, train and sustain the Engineer and IT workforce
- Develop and Mature Emerging Cybersecurity Technologies
- Harden the Networks and IT Systems Supporting Missions and Programs
- Enhance partnerships with Departments, Agencies' and the IC



IT Security Evaluation

NASA IT Security Center Program Data Call

- Goal is to provide a high level review of the maturity of the Center's IT Security program

- 10 focus areas
 - Information Security Program Management Gaps, Challenges and Culture
 - Effectiveness of Center Security Policies
 - Effectiveness of Regulatory Compliance Program (i.e. OMB, NIST, FISMA)
 - Effectiveness of Data Privacy Program
 - Effectiveness of Risk Assessment Lifecycle
 - Effectiveness of Metrics Program
 - Effectiveness of Employee Awareness Campaign
 - Effectiveness of Business Continuity and Disaster Recovery Program
 - Comprehensive Incident Response Process
 - Budget and Resources (Staffing)

- Completion by August 1, 2014



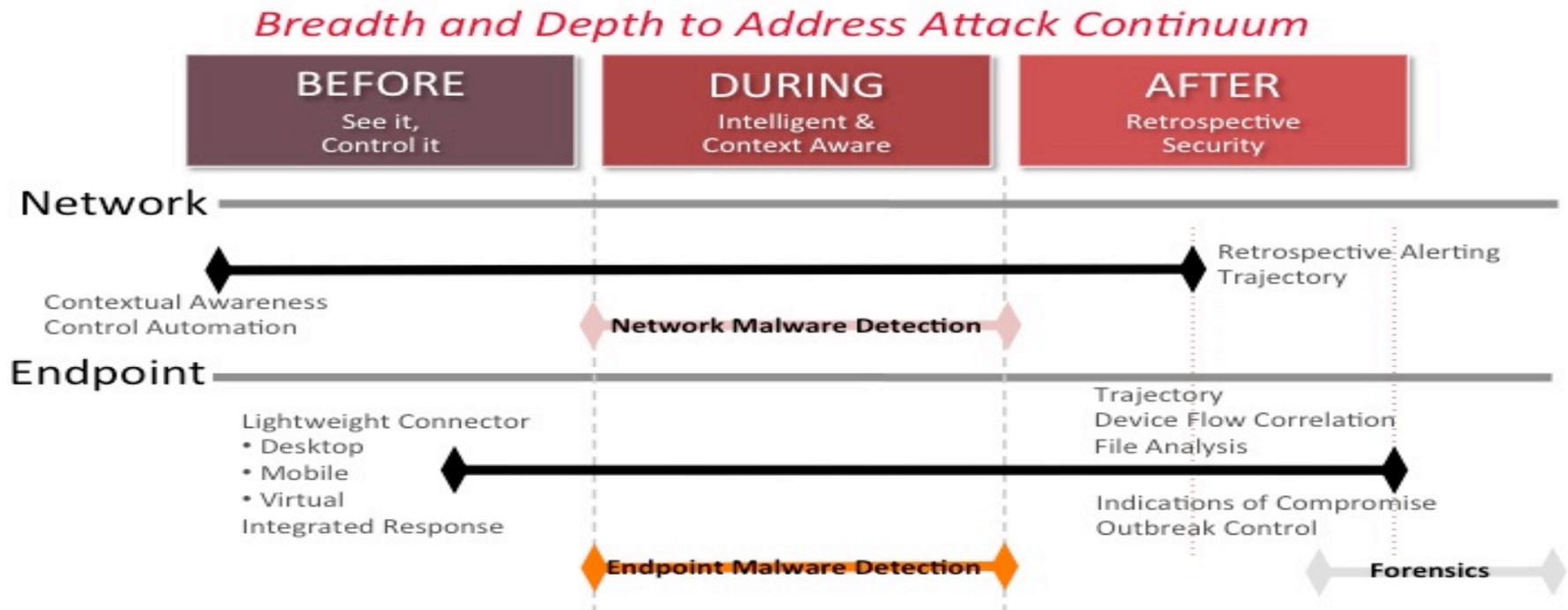
OCIO Next Steps

- **Improved security** at the data source
- **Internet of everything** – people, processes, things, data
- **Big Data and Data Analytics**
- **Mobility** – working from anywhere, anytime , and on any device
- **Leveraging Center capabilities** as an Agency service – not just 10 separate center services
- **OCIO becoming “brokers” and “consultants”** of all services





Future State Comprehensive and Integrated





IT Security

Legend:

Bold - MSC Funding
Bold [elevated] - MSC Funding Enhancement

Threat Management

Threat Management

Prevention

Monitoring / Detection

Containment / Eradication

Information Assurance

FY13-14 Capabilities

- Open Source
- US-Cert Incident Reporting
- Penetration Testing

- Data At Rest (DAR) / Disk Encryption
- Security Awareness & Training
- Patch Management (ASUS)
- Asset Configuration (ASCS)
- Web App. Secure Code Devlp. Training

- Anti-virus
- Anti-malware
- SOC Sec. Info. Event Mgmt. (SIEM)
- Network Forensics and Visibility
- ITSEC-EDW
- IDS
- Web Application Scanning

- Incident Response
- DNS Sink Hole
- IP Sink Hole
- NetMC
- Web App. Secure Code Repository

- Policy Development
- RMS / SA&A
- Privacy Program
- Sensitive Data Protection

FY14 Bundle 1

- Penetration Testing
- CI Threat Analysis
- AVAR
- SOC Malware Analysis

- Web App. Secure Code Devlp. Training
- IPS Implementation

- IDS Upgrade
- Web Application Scanning

- Web App. Secure Code Repository

FY15 Bundles 2&3, CDM

- Application Whitelisting
- Network Data Loss Prevention (DLP)
- End-User Data Loss Prevention (DLP)

- Web Application Firewall
- Next Generation Firewall
- SOC Life Cycle Refresh
- Configuration Management (CDM)
- Full Packet Capture (CDM)
- Dashboard System (CDM)

- SOC Cont. of Operations (SOC COOP)
- Cloud Security



Looking into the Future

Technology and Innovation Goals

■ Innovation and Digital Services

- Creating new opportunities for citizen engagement with challenge events like Space Apps, Earth Watch, and Space-A-Thon
- Test Bed Incubator to Operations (IT Labs)

■ Data Management and Services

- Planning in the works, considering new Office of Science and Technology Policy (OSTP) mandates for scientific information and publications

■ Enterprise Architecture

- Providing a consistent view across all program and service areas to support planning and decision-making

■ Emerging Technologies

- Bring Your Own Device (BYOD)

