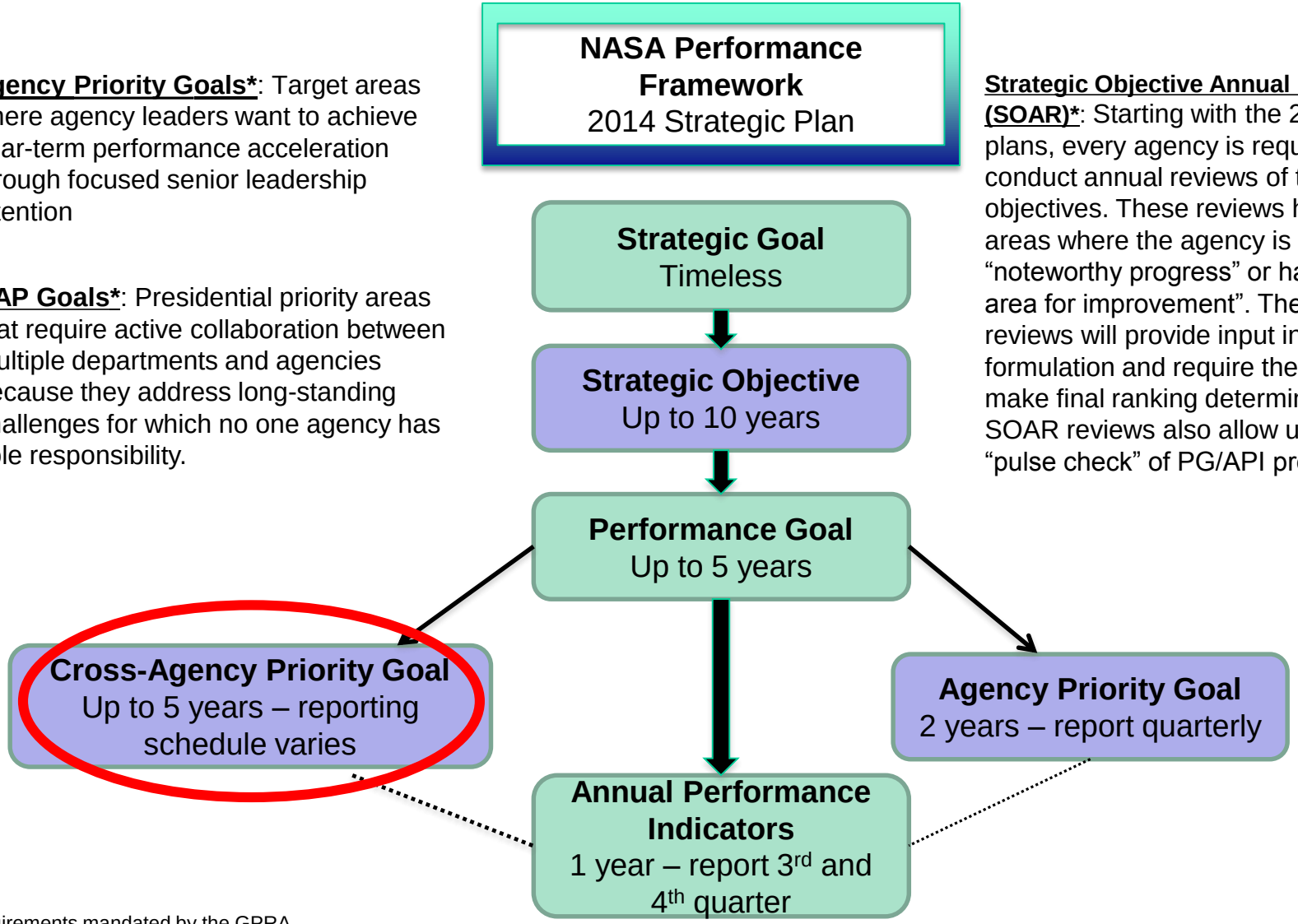
NASA Cybersecurity

March 27th, 2015

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

NASA Cybersecurity Continuous Monitoring Framework

Functions & Current Capabilities

FUNCTION	DESCRIPTION	CYBERSECURITY OUTCOMES	SERVICE AREAS	NASA'S CYBER PROGRAMS
Identify	Develop organizational understanding to manage cyber risk to systems, assets, data, and capabilities.	• Assets (equipment/ software/personnel) and interconnections are all Known/Managed • Vulnerabilities/Risks/Business Impacts are Known/ Managed • Roles/Responsibilities are clearly outlined • Budget is effectively managed and reported • Personnel management • Contract management	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Staffing resources • Budget planning	• IT Security Electronic Data Warehouse (ITSEC-EDW) • NASA Security Assessment & Authorization Repository • PCAT Support • Vulnerability Assessment • Governance Risk and Compliance • Cloud Security • NOC/SOC Integration • IT Security and Management Program • Resources and Planning Program
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services.	• Remote access uses strong authentication (PIV, 2-Factor) • Patch levels compliant with agency policy • Data at-rest and in-transit are protected • Protections against data leaks are implemented	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Agency Security Configuration Standards • IT Security Awareness & Training Center • Secure Web Coding Training • Upgrade to Next Gen Firewalls/Web Application Firewalls
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	• Assets (equipment/ software/personnel) and interconnections activity monitored (CDM) • Test exfiltration attempts are caught • Attempts to access large volumes of data detected/ investigated • All anomalies reported to SOC and US-CERT in accordance with Federal policy	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Agency Vulnerability Assessment & Remediation • Intrusion Prevention System • SOC Data Loss Prevention • Intrusion Detection System • SOC Continuous Monitoring • Network Data Loss Prevention • Web Application Security Program (WASP)
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	• Roles/Responsibilities are verified in incident response testing • Worst-case Incident Response Plan tested, updated within 30-days of test results • Established partnerships for surge resources/special capabilities (contracts/MOUs) • All contracts handling Sensitive Information contain clauses on protection/detection/ reporting of information loss	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Web Application Security Program • Penetration Testing • Network Forensics • Advanced Analytics • CI - Threat Analysis • Networks Forensics and Visibility
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cyber event.	• Business Continuity Plans are in place and fully tested for all levels of incidents • Recovery Plans incorporate lessons learned • Recovery activities are communicated to internal and external stakeholders • Ensure appropriate contingency plans are developed to compensate for mission impact of remediation efforts	• Recovery Planning • Improvements • Communications	• SOC COOP • Security Ops Center (SOC) Cont. of Operations Plan • SOC Life Cycle Refresh • ASUS Dell-Kace

NASA Federal Cybersecurity Self-Assessment:

Vulnerabilities & Self-Assessment Progress

Framework Functions	Function Description	Key Activities Completed/ Planned Actions for Next Quarter		Progress/ Risk Gap
Identify	Develop organizational understanding to manage cyber risk to systems, assets, data, and capabilities	**Completed**	• *RADAR ConOps language drafted to implement into agency policy*	Y
		Planned for Next Quarter	• *Additional testing of security settings for Mac V10.8 & V10.9 and RedHat V5 & V6* • *Clearly define asset management roles/responsibilities*	
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services	**Completed**	• *Completed Data-at-Rest encryption assessment across all NASA Centers* • *Perform weekly patching updates as defined in Agency policy*	Y
		Planned for Next Quarter	• *Progress towards all non-Windows 7 desktop solution for PIV compliance* • *Progress towards PIV access for privileged users*	
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	**Completed**	• *IDS deployed at TIC locations*	G
		Planned for Next Quarter	• *ITSEC-EDW and SOC will collaborate to ensure reporting to US-CERT*	
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	**Completed**	• *Incident Response tabletop exercise completed Q4FY14*	Y
		Planned for Next Quarter	• *Second Incident Response Plan test scheduled*	
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cyber event	**Completed**	• *Alternative Processing Site design*	Y
		Planned for Next Quarter	• *SOC COOP plans will be completed next quarter*	

- The Agency Self-Assessment is based upon agency performance and leadership judgment
- Focus is on progress and gap closures* using the criteria below to guide ratings

  Green: Agency shows progress and is on target to strengthen its cybersecurity posture or close all identified gaps

  Yellow: Agency shows progress and is on target to strengthen its position or close most identified gaps

  Red: Agency shows little progress and is not likely to close a majority of identified gaps

***For initial agency self-assessments**: Agencies were asked to use progress against the items outlined in the "PMC Cybersecurity Action" memo issued Sept. 16, 2014. For subsequent self-assessments, agencies have the latitude to add activities via the "Planned Actions for Next Quarter" portion of the "Agency Self-Assessment Template" to outline activities planned for the following quarter.

Phishing Exercise Update

Center	% of Opened Emails where the User Clicked the Link/Opened Attachment			
	Q3 FY14	Q4 FY14	Q1 FY15	Q2 FY15
ARC	29%	22%	5.5%	8.0%
AFRC	35%	31%	8.8%	9.0%
GRC	81%	38%	10.1%	7.5%
GSFC	55%	27%	6.9%	7.0%
HQ	60%	29%	6.5%	8.4%
JSC	51%	31%	8.2%	9.1%
JPL	N/A	N/A	N/A	4.2%
KSC	53%	35%	14.8%	10.0
LaRC	42%	24%	8.9%	5.8
MSFC	45%	28%	9.3%	10.8
NSSC	30%	42%	13.0%	8.4
SSC	50%	29%	10.3%	6.4
Total	**48%**	**29%**	**8.8%**	**8.0%**

Agency FY15 Goal	Performance	Trend
4%	R	Y

Trending patterns are difficult to compare as different attack techniques are used each quarter.

20% of Agency users were included in the phishing exercise conducted in February 2015.

Legend/Performance Change from Last Month: ⇨ **Unchanged** ⇧ **Improving** ⇩ **Declining**

Personal Identification Verification (PIV) Update

Agency FY 2015 Goal	OMB FY 2014 Cap Goal Target	Trend
75%	75%	R

Current Center Implementation	
Center	Phase 1 % Windows 7 Desktop Platforms w/ Smartcard Required Login (ECD March 31st, 2015)
AFRC	86.9%
ARC	84.0%
GRC	92.3%
GSFC	65.1%
HQ	89.5%
JSC	77.2%
KSC	97.6%
LaRC	84.0%
MSFC	95.1%
NSSC	83.9%
SSC	81.1%
NASA Total	84.1%
JPL	0.0% *

* JPL included in FISMA inventory reporting starting FY15.

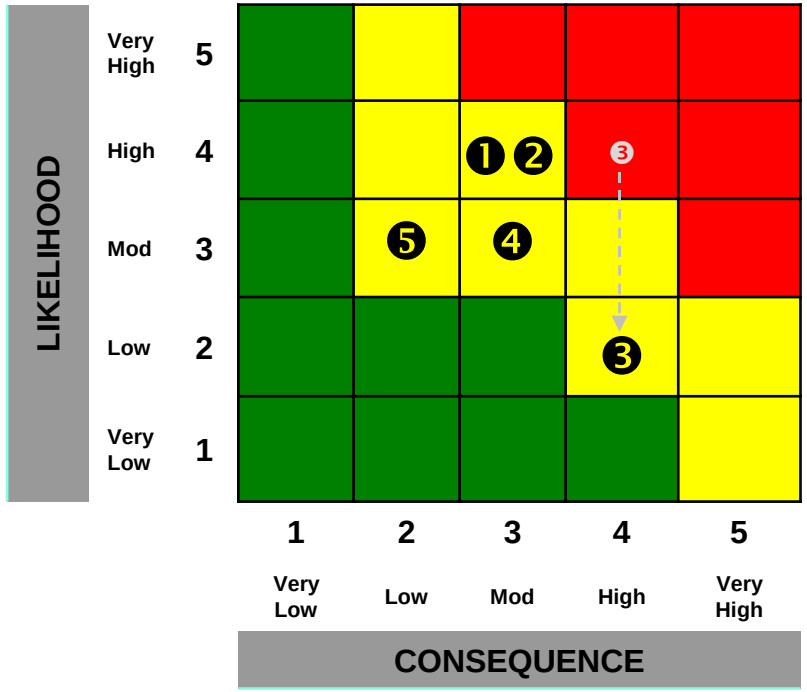
Enterprise Implementation			
	Phase 2 % All Windows/Mac/Unix/Linux Desktop Platforms w/ Smartcard Required Login (ECD Q4 FY16)	Phase 3 % All Windows/Mac/Unix/Linux Desktop Platforms Including Mobile Devices w/ Smartcard Required Login (ECD Q4 FY16)	Phase 4 % System Owners w/ Smartcard Required Login (ECD Q4 FY18)
NASA Total	62.1%	51.0%	0.0%

- FISMA/Cross-Agency Priority PIV goals require user account authentication metrics (Phase 4) rather than machine based metrics. The intent is to progress towards user-based enforcement.
- Current metrics will positively change as PIV solutions are addressed for non-Windows 7 desktop platforms.
- Validation of an industry solution for Mac/Unix/Linux systems will assist in the rollout of Phase 2.
- Derived credential implementation may assist in the rollout of Phase 3.
- Phase 4 rollout will require enterprise and local applications comply with mandatory smartcard login requirements.

Windows Platforms	8.x, 7.x, Vista, Unsupported (XP)

Legend/Performance Change from Last Month: ⇨ Unchanged ⇧ Improving ⇩ Declining

Risk Posture



Risk Seq.	Risk Name	Trend	Statement	Status M,W,R,C,A
1	Exfiltration of NASA Data	Y	If advanced threats, coupled with status quo network and data defense continue then the risk of NASA data exfiltration will increase to a very high likelihood and consequence rating.	**Mitigations:** • Quarterly Phishing Exercises • Intrusion Prevention Sys • Breach Prevention • Web Application Security Framework • Agency Security Perimeter
2	Social Engineering & Phishing	Y	If user education and border protection efforts digress then the risks associated with social engineering and phishing attacks will remain high.	**Mitigations:** • Quarterly Phishing Exercises • Intrusion Prevention Sys • Breach Prevention • Agency Security Perimeter
3	SOC Cont. of Operations Plan	Y	If central SOC services are disrupted, then central and comprehensive IT security incident detection and mitigation capabilities will cease.	**Mitigations:** • Completing the build-out of an alternative processing site for data analysis and storage. COOP is funded, now pending FAD approval.
4	Compromise of Agency Websites	Y	If web application protections and border protection efforts digress then the risks associated with website compromises will remain high.	**Mitigations:** • Intrusion Prevention Sys • Breach Prevention • Agency Security Perimeter • Web Application Security Framework
5	Compromise of User Accounts & Lost Devices	Y	If user education, system encryption, standardized authentication and border protection efforts do not continue to progress, risks associated with the compromise of user accounts and the impact of lost devices will increase.	**Mitigations:** • User Education • Data-At-Rest and PIV Authentication • Intrusion Prevention Systems • Breach Prevention

KEY

Risk Criticality	High (Red)		Medium (Yellow)	Low (Green)	
Status Codes	MITIGATE	WATCH	RESEARCH	ACCEPT	ELEVATE
Performance	Unchanged	Improving	Declining		
Risk Mitigation	1 Pre-Mitigation Risk - - → 1 Current Risk Status				

Legend/Performance Change from Last Month: Unchanged Improving Declining

NASA IT Security: Strengths/Weaknesses/Impacts

Strengths

15% lower number of findings (18) than industry average

Sound approaches to:

- App Dev Security
- Availability/Disaster Recovery
- Host/Platform Protection
- Access Management
- Data Integrity
- Monitoring
- Network Security
- Physical Security
- PKI/Encryption Use
- Vulnerability Management

Meeting or Exceeding Industry Trends in all areas except:

- Host/Platform Security
- Malicious Software Protection
- Monitoring

Large number of in-work initiatives reflects positive approach to security maturity

Weaknesses

60% of weaknesses are process-related, not technology

Large number of in-work initiatives reflect:

- Less than adequate current maturity
- Resource and priority drain

Organization/Culture Issues commensurate with enterprise program:

- Insufficient, infosec-dedicated resources
- Insufficient enforcement scope

Elevated risk areas due to reduced maturity:

- Change Management w/ Assurance
- Comprehensive Data Protection
- Endpoint Admission
- Security Governance approach
- Malicious Software Protection
- Mobile Security

Impacts

Process related issues limits enterprise security program to Reactive Posture: below minimum maturity level for due diligence.

Current weaknesses limit ability to comprehensively manage existing residual risk and proactively address emerging threats

Priorities for remediation:

- Security based change impact evaluation
- Protection for: removable media, databases, backups
- Access & configuration enforcement (IW)
- Resource study, governance committee, awareness & security plan enhancements
- Console alert management
- Mobile device management (IW)

In general, strengths, weaknesses, and in work initiatives reflect proactive approach

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.

NASA CIO

Office of the
Chief Information Officer