Fiscal Year 2018 -2019 FISMA Metrics

May 15, 2018

Craig Chase – DHS
craig.chase@hq.dhs.gov

Homeland
Security

FISMA 2014 Requirements

- ‘The Director (of OMB) shall oversee agency information security policies and practices….’
- ‘The Secretary (of DHS), in consultation with the Director (of OMB), shall administer the implementation of agency information security policies and practices for information systems, except national security systems…’
- ‘Not later than March 1 of each year, the Director (of OMB), in consultation with the Secretary (of DHS), shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year…’

Cyber Executive Order 13800

Policy:

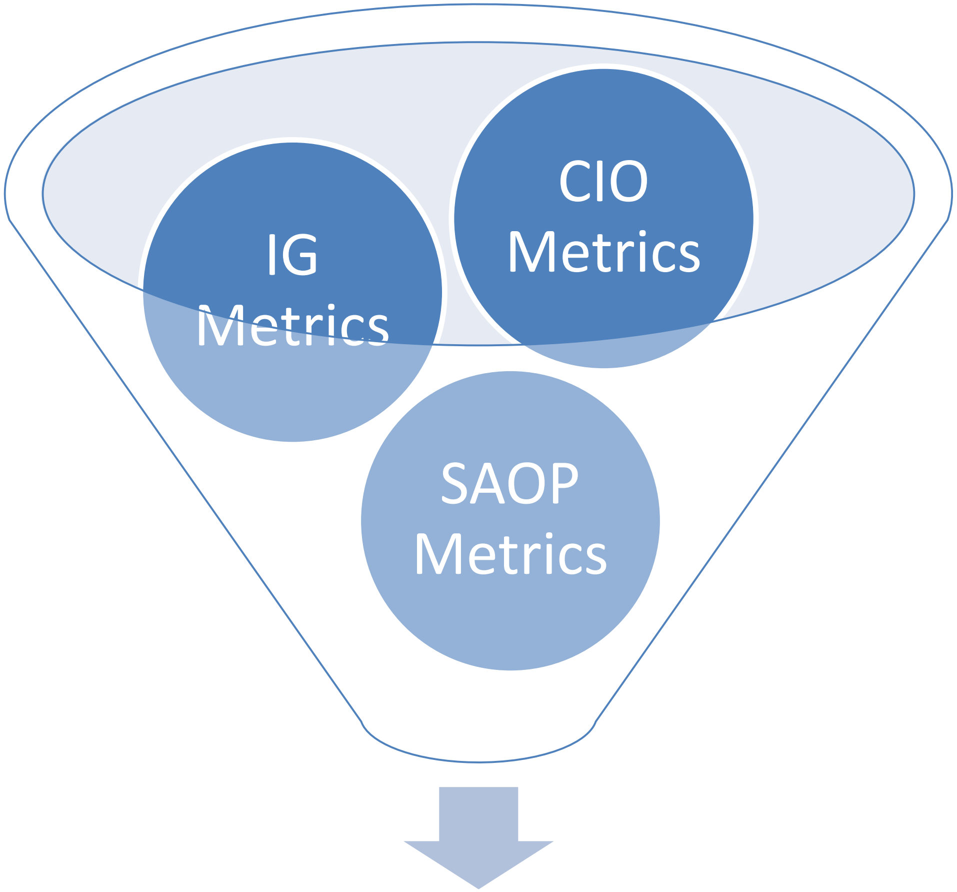
- ‘The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises.’

Risk Management:

- ‘Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code (FISMA 2014).’

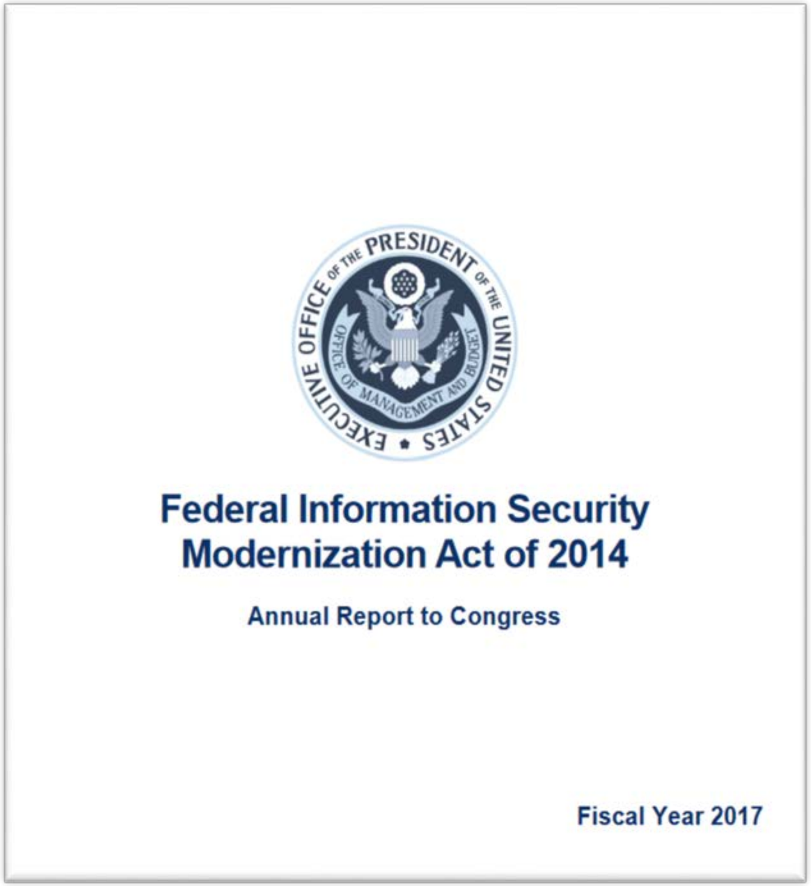
Source: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

FISMA Metrics Trilogy



FISMA Report to Congress
CAP Reports
Quarterly Risk Management Assessments
President's Management Council

FISMA Report to Congress



Federal Information Security Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2017

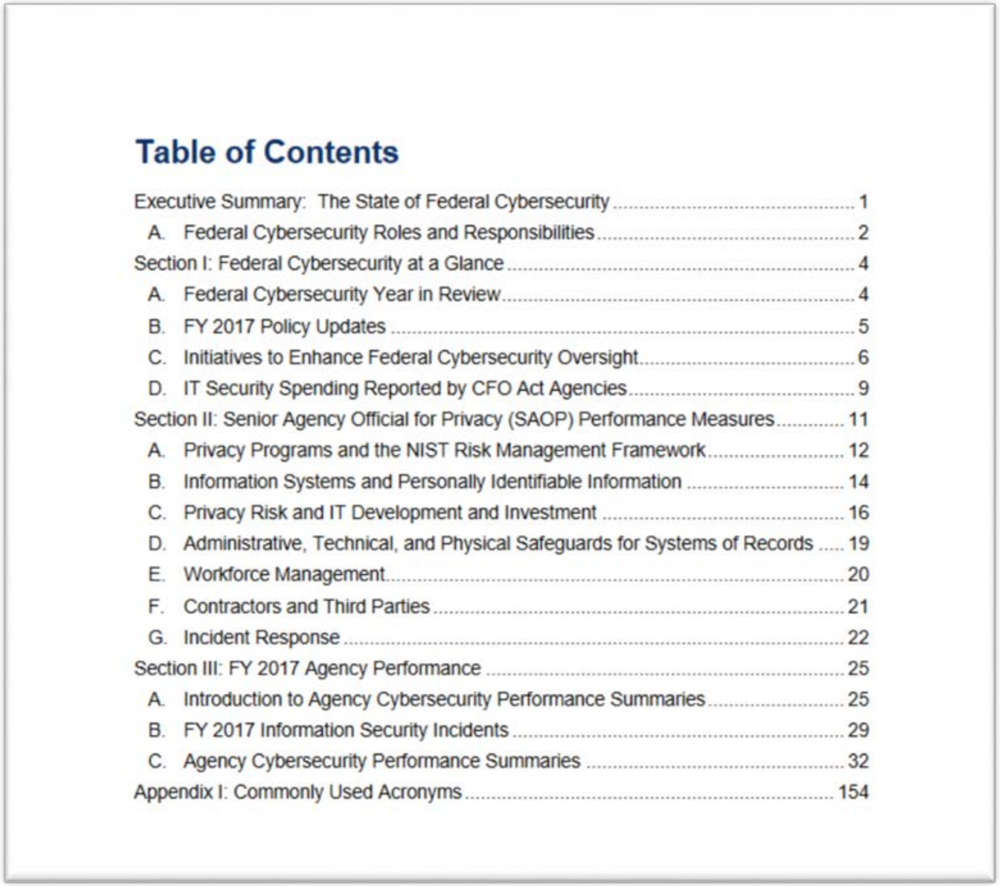


Table of Contents

Source: https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf

Agency Risk Management Assessment Results

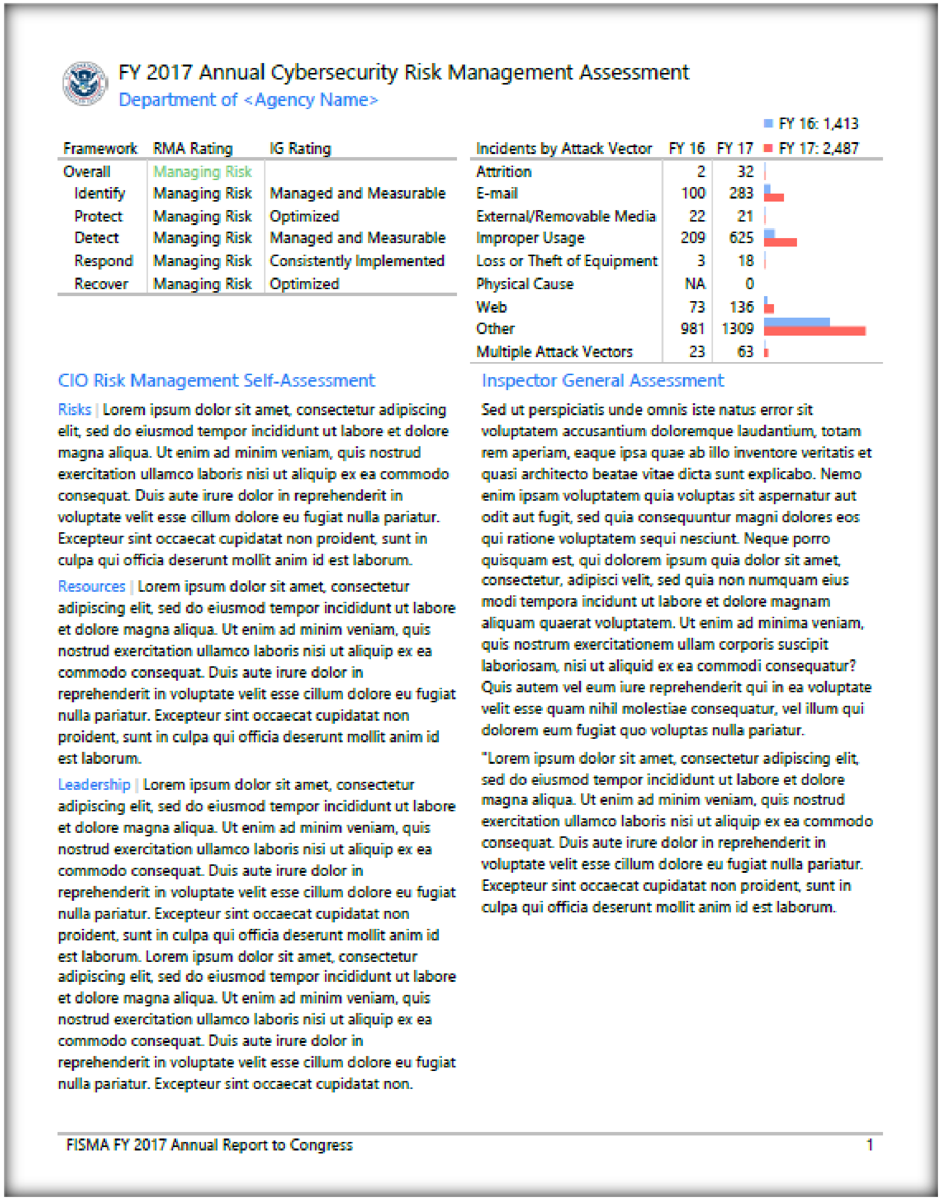
Number of Agencies	Risk
32	Managing Risk
58	At Risk
6	High Risk
Total Agencies: 96*	

*Excludes one Agency.

Source: https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf (pages 35-133)

Homeland Security

Sample Risk Management Assessment



FY 2017 Annual Cybersecurity Risk Management Assessment

Department of <Agency Name>

Framework	RMA Rating	IG Rating
Overall	Managing Risk	
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Optimized
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Consistently Implemented
Recover	Managing Risk	Optimized

Incidents by Attack Vector	FY 16	FY 17	🟦 FY 16: 1,413 🟥 FY 17: 2,487
Attrition	2	32	
E-mail	100	283	
External/Removable Media	22	21	
Improper Usage	209	625	
Loss or Theft of Equipment	3	18	
Physical Cause	NA	0	
Web	73	136	
Other	981	1309	
Multiple Attack Vectors	23	63	

CIO Risk Management Self-Assessment

Risks | Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Resources | Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Leadership | Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non.

Inspector General Assessment

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur.

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

FISMA FY 2017 Annual Report to Congress 1

CIO
Metrics

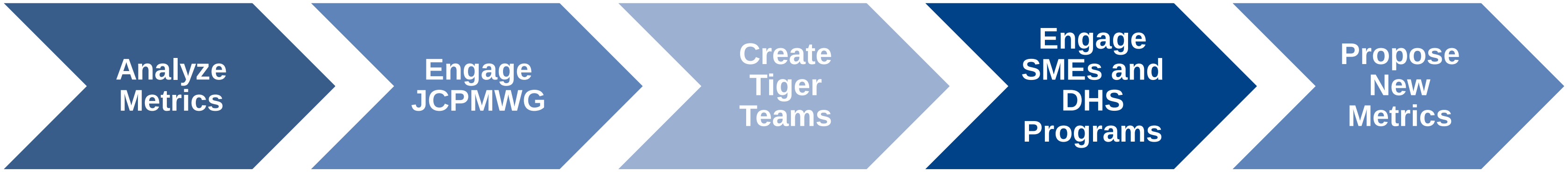
Chief Information Officer Metrics

Purpose and Process: FY 2018 CIO Metrics Mid-Year Update

CIO Metrics

Executive Order (EO) 13800 and the *Report to the President on Federal IT Modernization* called for increased stakeholder engagement to collaborate with the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) to shape more effective metrics beginning in FY 2018 which:

- Measure and provide awareness of department and agency (D/A) cybersecurity program maturity,
- Solicit outcomes that inform risk acceptance decisions and steer budget and resource allocation,
- Incrementally improve on current metrics,
- Alleviate the reporting burden on D/As, and
- Address High Value Assets (HVA).


Analyze Metrics → Engage JCPMWG → Create Tiger Teams → Engage SMEs and DHS Programs → Propose New Metrics

Summary of Revisions to FY 2018 CIO Metrics

CIO Metrics

Revision	Outcome
Proposed move of policy-based metrics to Inspector General (IG) Metrics.	Highlight existence and effectiveness metrics in a qualitative format through IG reporting for better insight into performance.
Re-worded metrics, removed duplicative metrics, and provided additional definitions as needed.	Provide additional clarity and understanding for stakeholders.
Highlighted metrics that involved mobile devices.	Provide insight into mobility challenges and separate from other means of asset management.
Removed metrics with no use case and reuse data from authoritative sources (e.g. Binding Operational Directives (BOD)).	Reduce duplication and streamline metrics by aligning to authoritative data sources.
Improved alignment of metrics language to a standard cybersecurity taxonomy.	Focus on commonality with standards such as Cybersecurity Framework (CSF) and OMB/NIST/DHS efforts that assist Agencies.
Introduced agency mission essential functions through focus on HVA metrics.	Introduce cybersecurity risk management and prioritization through high value asset focus.

Summary of FY 2018 CIO Metrics Update Results

CIO Metrics

Results	# of FY 2018 Metrics	# of Added Metrics	# of Modified Metrics	# of Removed Metrics	# of Updated FY 2018 Metrics
Identify	22	2	8	(6)	18
Protect	51	3	18	(17)	37
Detect	17	0	12	(3)	14
Respond	12	1	3	(7)	6
Recover	9	1	2	(7)	3
Total	111	7	43	(40)	78

*The total number of revised FY 2018 CIO Metrics represents a **30% decrease** from the total number of FY 2018 CIO Metrics total.*

Rationale for Metrics Improvement

CIO Metrics

- Issue: Metrics development is a one-time activity
  - **Solution**: Metrics development will be an iterative process supporting a long-term vision that focuses on adaptive measures, risk management, and continuous improvement.
- Issue: Stakeholders are not continuously engaged
  - **Solution**: Leverage ongoing engagement with the Joint Cybersecurity Performance Management Working Group (JCPMWG), a resource to help develop the metrics for reporting and focus on improving decision making for stakeholders aligned with vision statement. Identify additional customers that can benefit from DHS products.
- Issue: Data collection is not automated or aggregated
  - **Solution**: Consolidate and leverage data collected from DHS services and other Federal sources, including Federal budgets and information collected by DHS, NPPD CS&C. Reuse data already collected and provide insight through analytics.

Plan for FY 2018 and Beyond

CIO Metrics

Outcomes

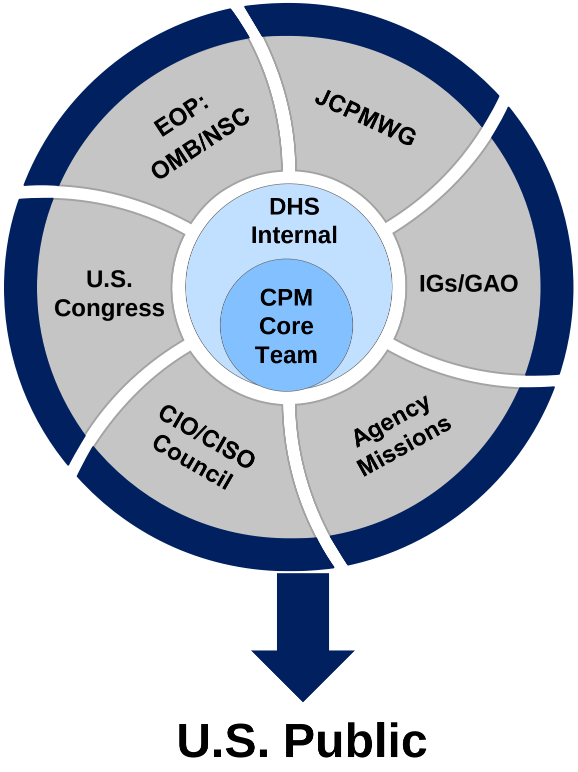
- Real-time agency mission risk management decision making.

Output

- Standardize metric reporting and utilization across Federal Government cybersecurity initiatives (e.g., .BOD, CSF, CDM).
- Automation of metrics.
- Secure agency mission data.

Value

- The ability to provide actionable and timely cybersecurity performance information to all Federal missions.



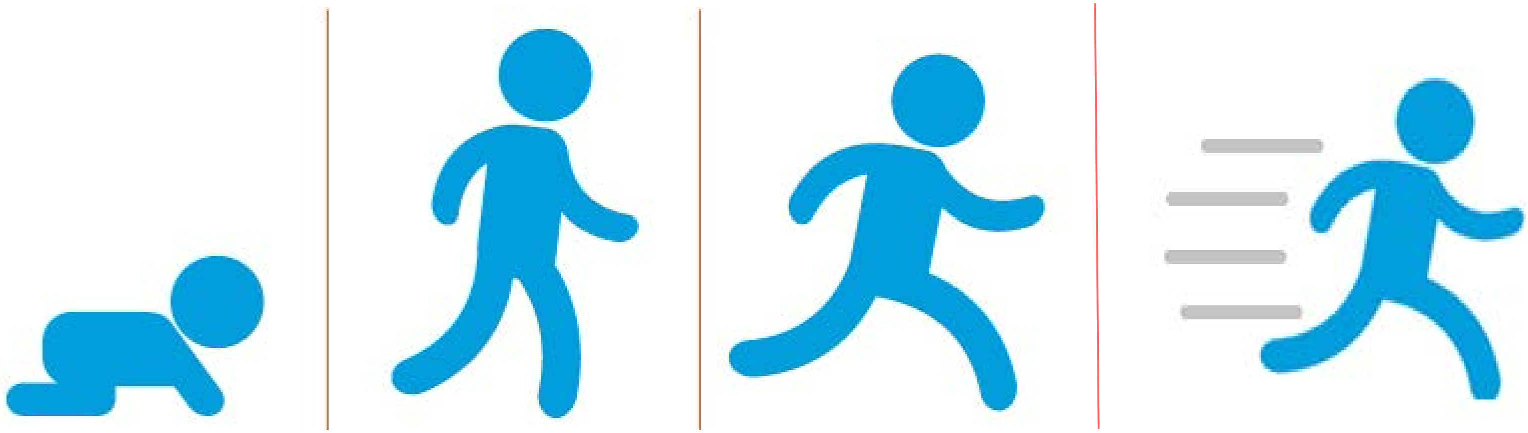
Plan for FY 2018 and Beyond (cont.)

CIO Metrics

Dates	Focus	Activities
Feb – Sept 2018)	**Roadmap**	**Quick wins to set up basis for long term vision:** ☑ Update FY 2018 Annual CIO Metrics with alignment to .govCAR, Cross-Agency Priority (CAP) Goals, and Outcomes. ☑ Where possible, tie IG, CIO, Senior Agency Official for Privacy (SAOP) metrics to performance measurement. ☑ Map various frameworks and capabilities for gap analysis (Risk, Threat). □ Finalize measures improvement implementation model, implement one NIST CSF function area. □ Develop FY 2019 Annual CIO Metrics. □ Begin the build out of the Business Data Model.

FY 2018 and beyond

CIO Metrics



2018-2019: Roadmap

2020: Process

2021: Timely Measurement

2021+: Continuous Improvement

Vision Statement

In 2021, cybersecurity data elements will inform timely performance measurement, providing mission stakeholders with information to improve cybersecurity business decisions.

IG
Metrics

Office of Inspector General Metrics

SAOP
Metrics

Senior Agency Official for Privacy Metrics

Questions and Resources

- DHS FISMA Website (all current and historical metrics are posted here)
  - www.dhs.gov/fisma

- FNR FISMA Team
  - FNR.FISMA@hq.dhs.gov

- CyberScope Help Desk
  - CyberScopeHelp@hq.dhs.gov

- CyberScope Max Portal Page
  - https://community.max.gov/x/hQIJL