National Science Foundation National Science Board Audit and Committee on Oversight Fiscal Year 2019 Audit Results

November 19, 2019

Presented by David Zavada (Senior Partner) and Phil Moore (IT Partner)

KEARNEY& COMPANY

KEARNEY & COMPANY

Agenda

- Scope
- Results
- Looking Forward
- Engagement Team
- Appendix A: Levels of internal control findings
- Appendix B: Current Year Internal Control Notifications of Findings and Recommendations (NFR)
- Appendix C: Current Year Non-Compliance NFRs

Scope

Engagement Scope of Work:

- Conducted an audit of the National Science Foundation's (NSF) financial statements for the fiscal year (FY) ended September 30, 2019
  - Assessed NSF's information technology (IT) control activities based on the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM) with IT controls related to the generation of financial statements
- Conducted a performance audit of NSF's information security program in accordance with the *Federal Information Security Modernization Act of 2014* (FISMA):
  - Prepared responses to the Department of Homeland Security's (DHS) *FY 2019 Inspector General (IG) FISMA Reporting Metrics*.

Scope

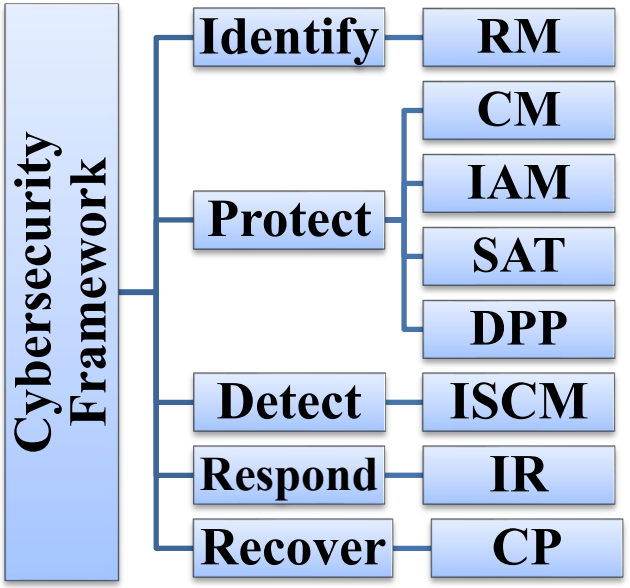
Engagement Scope of Work (Con't):

- Conducted a performance audit of NSF's FY 2019 compliance with the Digital Accountability and Transparency Act of 2014 (DATA Act) requirements, in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) / Federal Audit Executive Council (FAEC) FY 2019 Inspector General Guide to Compliance under the DATA Act (February 2019)

Scope

What is FISMA?

- What is the Federal Information Security Modernization Act (FISMA)?
  - Congress mandates that every Federal agency will carry out a cyber security audit of their information security programs and practices
  - FISMA uses a maturity model concept to assess Federal Information Security Programs using the NIST Cyber Security Framework and NIST SP 800-53
  - The DHS FY2019 IG FISMA Reporting Metrics define "Effective" as level 4 (Managed and Measurable)



Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
Policies and procedures are not formalized	Policies and procedures are defined but not consistently implemented	Policies and procedures are consistently implemented, but lack quantitative and qualitative effectiveness measures	Quantitative and qualitative effectiveness measures are collected and used across the organization	Policies and procedures are fully institutionalized, repeatable, automated where appropriate, consistently implemented, and regularly updated

FISMA-001

Results

Results of Work:

- Independent Auditor's Report
  - Unmodified opinion on the NSF's FY 2019 financial statements
- Independent Auditor's Report on Internal Control Over Financial Reporting
  - No material weaknesses
  - No significant deficiencies
- Report on Compliance and Other Matters
  - No instances of noncompliance
- Report on NSF's Information Security Program for FY 2019 (FISMA report):
  - Overall assessment of "Not Effective" based on DHS *FY 2019 IG FISMA Reporting Metrics* maturity model
    - Maturity ratings are scaled from Level 1 (Ad Hoc) to Level 5 (Optimized).
    - Metrics define "Effective" as Level 4 (Managed and Measurable); NSF was rated at Level 3 (Consistently Implemented)

Results (cont'd)

Results of Work (cont'd):

- DATA Act Performance Audit Report
  - Developed and submitted recommendations to NSF's implementation of the DATA Act standards to further enhance the completeness (57.5% error rate), accuracy (57.5% error rate), and timeliness (57.7% error rate) of data as part of its quarterly submission process.
    - The majority of discrepancies were File C (Award Financial Data) transactions not reported in File D2 (Award Financial Assistance), which resulted from NSF's interpretation of the DATA Act reporting guidance which differed from Kearney's interpretation
    - The discrepancies extended across all data elements resulting in a determination of low data quality; however, NSF's presumed error rate if the File C to D2 errors were removed would likely be minimal.

KEARNEY & COMPANY

Looking Forward

- Financial Statement Audit (including FISCAM/FISMA)
  - Coordinate and schedule meetings to discuss the planning and implementation of corrective actions for Management Letter comments so they do not become future significant deficiencies.
- DATA Act
  - Hold upcoming meeting/discussion (tentatively December 2019) regarding deficiencies noted to reach common ground and clarify corrective action plans going forward.

KEARNEY & COMPANY

Engagement Team

Key members of the FY 2019 Engagement Team:

- Partners/Principals
  - David Zavada, CPA – Engagement Partner (Overall Responsibility)
  - Phil Moore, CPA, CISA, PMP – IT Partner
  - William Kubistal, CPA, CISA – Quality Control (QC) Partner
  - Sarah Allen, CPA, CGFM, CISA – Financial Audit Principal
- Team Leads
  - Marcos Vigil – Financial Audit Lead
  - Eric Pennington, CISA, PMP – IT Audit Lead
- Audit Manager
  - Nupur Moondra – Financial Audit Manager

KEARNEY& COMPANY

Questions?

KEARNEY & COMPANY

Appendix A: Levels of Internal Control Findings

Results of Work:

- Levels of internal control findings
  - **Material weakness** – is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.
  - **Significant deficiency** – is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.
  - **Deficiency** (Management Letter comment) – findings and recommendations for improvements in internal control, which were identified during the audit, but were not required to be included in the auditor's report on internal control over financial reporting or report on compliance and other matters.

KEARNEY & COMPANY

Appendix B: Current Year Internal Control NFRs

NFRs Issued (Financial): Management Letter Comments

- NFR #1 – Enhance Monitoring and Oversight over Undelivered Orders (Modified Reissue)
- NFR #2 – Payroll Oversight over Separation Actions (Modified Reissue)
- NFR #3 – Inadequate Accounts Payable Accrual Validation Methodology (New)
- NFR #4 – Internal Control Program Needs Improvement (New)
- NFR #5 – Inadequate Monitoring over Manual Small Business Innovation Research (SBIR) Grants Undelivered Orders (New)
- NFR #6 – Insufficient Monitoring and Oversight over Construction in Progress Accrual Estimation Process (New)
- NFR #7 – Insufficient Monitoring and Oversight over Property Plant, and Equipment (PP&E) U.S. Antarctic Program (USAP) related Activities (New)
- NFR #8 – Accounts Payable Accrual Validation Errors (New)

KEARNEY & COMPANY

Appendix B: Current Year Internal Control NFRs (cont'd)

NFRs Issued (IT FISCAM): Management Letter Comments

- NFR #1 – Awards Operating System (OS) and Database (DB) Audit Logging (New)
- NFR #2 – Awards OS and DB Service Account Monitoring (New)
- NFR #3 – Awards Application User Authorization (New)
- NFR #4 – Awards DB Patch Management (New)
- NFR #5 – WebTA Application User Access Issues (New)
- NFR #6 – Service Organization Monitoring (New)

KEARNEY & COMPANY

Appendix C: Current Year Non-Compliance NFRs

NFRs Issued (IT FISMA): Non-Compliance Findings

- NFR #1 – USAP Directives Not Reflective of Current National Institute of Standards and Technology (NIST) Requirements (New)
- NFR #2 – General Risk Management (New)
- NFR #3 – General Configuration Management (New)
- NFR #4 – Baseline Configuration and Vulnerability Management (New)
- NFR #5 – NSF Screening Process (New)
- NFR #6 – Authentication and Identification (New)
- NFR #7 – Incident Response Tool (New)

KEARNEY & COMPANY

Appendix C: Current Year Non-Compliance NFRs (cont'd)

NFRs Issued (DATA Act): Non-Compliance Findings

- NFR #1 – Incomplete Record-Level Linkage from File C (Financial) to File D2 (Award – Financial Assistance) (New)
- NFR #2 – Incomplete Record-Level Linkage from File C (Financial) to File D1 (Award – Procurement) (New)
- NFR #3 – Inaccurate Reporting of Data Element within the System for Award Management (New)