



**National Science Foundation  
National Science Board Audit and  
Oversight Committee  
Fiscal Year 2020 Audit Results**



**KEARNEY &  
COMPANY**

*December 9, 2020*

- In response to the Safety Protocols Related to the Coronavirus 2019 (COVID-19) global pandemic:
  - Travel was halted and all audit observations were held remotely
  - Minimal delays/difficulties were related to obtaining audit evidence (some documentation was held in the NSF office)
  - Meetings, walkthroughs, and observations were held efficiently and effectively over Zoom, Microsoft (MS) Teams, e-mail, phone, etc.
    - We were able to capture some audit evidence on the spot without additional Provided by Client (PBC) requests through screenshare processes
  - Vulnerability testing was adequately assessed through agreed-upon “shoulder surfing” instead of onsite scanning

- Report on the National Science Foundation's (NSF) financial statements
  - Unmodified Opinion
- Report on Internal Controls over Financial Reporting
  - No Material Weaknesses
  - No Significant Deficiencies
- Report on Compliance with Applicable Provisions of Laws, Regulations, Contracts, and Grant Agreements
  - Including compliance with the applicable provisions referred to in the Federal Financial Management Improvement Act of 1996 (FFMIA)
  - No instances of reportable non-compliance noted.

**Results of Work:**

- Report on NSF's Information Security Program for FY 2020 (FISMA report):
  - Overall assessment of “Effective” (Level 4) based on Department of Homeland Security's (DHS) *Fiscal Year (FY) 2020 Inspector General (IG) FISMA Reporting Metrics* maturity model
    - Maturity ratings are scaled from Level 1 (Ad Hoc) to Level 5 (Optimized).
  - NSF has taken steps to implement corrective action plans based on FY 2019 findings and recommendations, although we identified areas for improvement. The related conclusions for all 5 domains are below:
    - Identify – Effective
    - Protect – Effective
      - Data Protection and Privacy (DPP) – Ineffective
    - Detect – Effective
    - Respond – Effective
    - Recover – Effective

## **NFRs Issued (Financial):**

- NFR #1 – Insufficient Oversight over Payroll Separated Actions (Modified Repeat)
- NFR #2 – Inadequate Monitoring and Oversight over Small Business Innovation Research (SBIR) Undelivered Orders (UDOs) (Modified Repeat)
- NFR #3 – Inadequate Accounts Payable Accrual Validation Methodology (Modified Repeat)
- NFR #4 – Insufficient Controls over New Hire Payroll Personnel Actions (New)
- NFR #5 – Insufficient Monitoring and Oversight over Property, Plant, and Equipment (PP&E) United States Antarctic Program (USAP) (Modified Repeat)
- NFR #6 – Insufficient Controls over Recording Internal Property Transactions (New)
- NFR #7 – Insufficient Control over Property in the Custody of Others (New)

## **NFRs Issued (IT Financial):**

- NFR #1 – Awards Cash Management Service (ACM\$) and MyNSF OS and DB Audit Logging (New)
- NFR #2 – MyNSF Timely Access Termination (New)
- NFR #3 – WebTA Application Recertification (New)
- NFR #4 – ACM\$ and MyNSF OS and DB Service Account Monitoring (New)
- NFR #5 – Review and Analysis of Invoice Processing Platform (IPP) Service and Sub-Service Organizations (Modified Repeat)

## **NFRs Issued (IT FISMA):**

- NFR #1 – NSF Report Server PII Access (New)
- NFR #2 – USAP Implementation of Incident Response Tool (SIEM) (Modified Repeat)
- NFR #3 – USAP Personal Identify Verification (PIV) Implementation (Modified Repeat)
- NFR #4 – USAP Screening Process (Modified Repeat)
- NFR #5 – Baseline Configuration (New)
- NFR #6 – ACM\$ and MyNSF Operating System (OS) and Database (DB) Audit Logging (New)
- NFR #7 – MyNSF Timely Access Termination (New)
- NFR #8 – ACM\$ and MyNSF OS and DB Service Account Monitoring (New)

FY 2019	Finding Description	FY 2020 NFR Status
2019-FR-01	Enhance Monitoring and Oversight over Undelivered Orders (UDO)	Closed
2019-FR-02	Insufficient Oversight over Payroll Separated Actions	Modified Reissue 2020-FR-01
2019-FR-03	Inadequate Accounts Payable (AP) Accrual Validation Methodology	Modified Reissue 2020-FR-03
2019-FR-04	Internal Control Program Needs Improvement	Closed
2019-FR-05	Inadequate Monitoring and Oversight over Small Business Innovation Research (SBIR) UDOS	Modified Reissue 2020-FR-02
2019-FR-06	Insufficient Monitoring and Oversight over Construction in Progress (CIP) Accrual Estimation Process	Closed
2019-FR-07	Insufficient Monitoring and Oversight over Property, Plant, and Equipment (PP&E) United States Antarctic Program (USAP)	Modified Reissue 2020-FR-05
2019-FR-08	AP Accrual Validation Testing Inaccuracies and Results	Closed



<b>FY 2019</b>	<b>Finding Description</b>	<b>FY 2020 NFR Status</b>
2019-IT-01	Awards Operating System (OS) and Database (DB) Audit Logging	Closed
2019-IT-02	Awards OS and DB Service Account Monitoring	Closed
2019-IT-03	Awards Application User Authorization	Closed
2019-IT-04	Awards DB Patch Management	Closed
2019-IT-05	WebTA Application User Access Issues	Closed
2019-IT-06	Review and Analysis of Invoice Processing Platform (IPP) Service and Sub-Service Organizations	Modified Reissue 2020-IT-05

NFR Reference	Finding Description	FY 2020 NFR Status
FISMA 2019-01	USAP Directives Not Reflective of Current NIST Requirements	Closed
FISMA 2019-02	General Risk Management	Closed
FISMA 2019-03	General Configuration Management	Closed
FISMA 2019-04	Vulnerability Management	Closed
FISMA 2019-05	Screening Process	Modified Re-issue FISMA 2020-04
FISMA 2019-06	Authentication and Identification	Modified Re-issue FISMA 2020-03
FISMA 2019-07	Incident Response Tool	Modified Re-issue FISMA 2020-02