BOAC Subcommittee on NSF’s Information Technology and Enterprise Architecture Recommendations—March 2024

Introduction

The BOAC IT Subcommittee has reviewed NSF's IT Strategy and related architecture plans and is providing a list of informed recommendations for changes in process, direction, and potential investment in new and emerging technologies for possible implementation in the next budget year.

Subcommittee members were unanimous in their belief that significant progress has been made by the CIO's office on the 2022 BOAC recommendations. In particular, the alignment of the OCIO operating structure to the government-wide OCIO operating model is noted. These improvements should be made clear to partners across government.

The CIO has prioritized six core IT functions and recognizes four strategic opportunities: Digital Experience, Artificial Intelligence, All-in on Zero Trust, and Data-as-a-Service. The CIO characterized each of these core functions and strategic opportunities in terms of their maturity and resource levels.

The Subcommittee’s four 2023 recommendations focus on the key areas within the CIO’s priorities that are most impactful to the success of all the OCIO’s strategies and core functions and require the CIO’s focused attention in 2024. The Subcommittee's recommendations are designed to provide a framework from which the CIO can reasonably set the stage for long-term success while maintaining core IT capabilities that NSF requires for mission success.

The Subcommittee’s primary guidance to the OCIO is: Emphasis must be placed on establishing an appropriate balance between NSF-wide initiatives and maintaining OCIO core IT functions. A special focus should be on stakeholder engagement, including the establishment of an Intra-Agency IT Committee devoted to the responsible use of emergent technologies and Federal IT policies.

Priority Areas for Recommendations

1. **The OCIO should fundamentally restructure its culture and relationships with NSF Directorates and external partners by building a Stakeholder Engagement Core Function for both internal and external customers. This will lead to an alignment of OCIO’s strategies and resource allocation decisions to NSF’s mission and business process. Emphasis needs to be placed on establishing an appropriate balance between NSF priorities/core IT functions, prioritization, and the importance of each.**

   1.1 Develop a strategic planning and stakeholder engagement process to understand IT requirements within NSF, with a specific focus on emergent requirements that span all NSF Directorates, such as AI and cybersecurity.

   1.2 Create a consumable view of NSF’s IT budget, including how the OCIO’s budget can supplement and support Directorate IT budgets and how budget responsibility or funds management will shift. Communicate this across the Agency for current and future budgets to ensure that momentum on key initiatives continues even if funding or primary oversight responsibility shifts.

1.3 Redefine key interaction points inside and outside of NSF under a new working model. Define expectations (both ways) and specific communication channels/protocols. This will ensure that there is clarity about new operating processes and ensure communications flow between appropriate parties per new roles and responsibilities.

2. **OCIO should establish its own AI Innovation Center to build and iterate on end-to-end AI development (both commercial off-the-shelf and In-house development) in order to ensure efforts align with the recent AI Executive Order and reflect its core themes around trustworthy and responsible AI and risk management. The Center would also align rapidly to emerging policy, data standards, and NSF technical architecture standards, and enable NSF to adapt to continuously evolving AI technologies.**

2.1 Align a continuous upskilling strategy with the pace of AI and data technology. Develop a strategy to educate the data science community, including citizen developers, and to continually train the workforce on generative AI, policy, and any new AI developments to empower them to identify and implement valuable AI deliveries to improve experiences and efficiency.

2.2 Dedicate resources for prototyping. Have an intentional budget for exploration (including for generative AI) for internal and off-the-shelf development. Adapting Generative AI for NSF will require customizing foundation AI model(s) based on NSF knowledge sources and budget allocations (for technology and human resources) for initial development and continued maintenance to ensure NSF's AI deployments stay current without getting stale.

2.3 Define AI inspection/verification processes per proposed government operating model at the Agency level service for efficiency of costs and pace. As AI deliveries progress from discriminative to generative, verification of results requires intentional effort to ensure it scales effectively for the variety of use cases. NSF could utilize generative AI deliveries for content generation, extraction, summarization, upgrading search and more. A standard verification process will help the developers deploy these efficiently while ensuring it meets quality and ethical requirements. NSF should consider sharing their learnings with other agencies with authorities in this space.

2.4 Ensure NSF policies apply to all AI use cases within NSF. NSF's AI policy has exceptions for its merit review process, common commercial products, and some use cases within the NCSES. Even if there are reporting limitations, all use cases need to apply to the principals and practices set forth by NSF. If needed, policies should be expanded to clearly handle the exceptions (stating how they will comply, even if not being reported).

3. **Focus on IT governance via a realigned Agency IT Decision Framework that is consistent with the OCIO's new roles and responsibilities. Create NSF-wide IT policies and standard operating procedures (SOPs) that build on current OCIO-centric policies and SOPs to establish a common view that is accepted by the Directorates and is understandable to citizens. This Framework should include AI policies, data inventories, code inventories, cybersecurity policies (including supply chain), records management, privacy, etc.**

   3.1 Creation of an NSF intra-agency IT Committee devoted to the responsible use of emergent technologies and Federal IT policies. The IT Committee would develop standards for AI policies and adoption, FISMA, data inventories, code inventories, cybersecurity policies (including supply chain), records management, privacy, and other areas identified by the CIO as critical to the functioning of NSF.

   3.2 For AI and cybersecurity, OCIO should take the lead to set SOPs, policies and adoption practices. These two areas span every aspect of NSF business processes and mission delivery and should be used by the OCIO to demonstrate clear value through thought leadership practices that touch on merit review processes, privacy concerns and other NSF-wide issues.

   3.3 OCIO should develop a common data dictionary when looking at data assets across the Agency—FISMA, security, data catalog, records management, and privacy assessments should all be mapping back to a common inventory; and make necessary enhancements for data provenance.

4. **OCIO should propose actions to ensure proper end-to-end security in the merit review process in order to protect the integrity of intellectual property and national assets created in the research process. Inform mission areas of gaps and opportunities to close gaps through technology and/or process. Enable the research community to adopt NSF-mandated secure platforms through strong partner engagement to increase transparency and control of the data.**

   4.1 Seek opportunities to mature the security of the end-to-end merit review/grants management process and consider leveraging best practices from other Federal agencies.

   4.2 Provide technical support for NSF to gain more secure and transparent data from research to results.

   4.3 Continue evaluating opportunities for shared services with other Federal agencies.

   4.4 Consider enhancements in technology and process expectations to include:

      4.4.1 Integrate cybersecurity capabilities into the grants workflow.

      4.4.2 Ensure grantees understand the IT security expectations that the government expects to make use of any products or data that is generated.

      4.4.3 Grantees should expect that they could be inspected/audited and action taken if security protocols are not meeting expected standards.