



OGM Work Plan FY18

Operational Services

The DOS submission for the FY 18 OGM Work Plan is provided below. A number of new requirements have been added to satisfy compliance with new and ongoing initiatives. The team will focus on managing electronic records, implementing the requirements of federal Continuity Directive-2, and bolstering the Board's Occupational Health and Safety Program. It will also focus on building the personnel security program and bringing the Insider Threat Program to Full Operating Capability. Finally, the team will focus on the continued effort to improve the protection of classified and sensitive information.

1. **Records Management (Mandatory)**

CAPSTONE Implementation. The Presidential Memorandum on Managing Government Records required agencies to manage both permanent *and* temporary email records in an accessible electronic format by December 31, 2016. To bring the agency into compliance with NARA requirements, OGM will implement the approved CAPSTONE approach to managing e-mail records during FY18.

2. **Facilities, Emergency Management and Occupational Health and Safety (Mandatory)**

a. Federal Continuity Directive-2 (FCD-2). FCD-2 requires agencies to validate Mission Essential Functions (MEFs). The validation includes conducting a comprehensive Business Process Analysis to understand processes necessary to perform organizational functions and requirements. It also includes conducting a Business Impact Analysis to identify potential impacts on the performance of essential functions and the consequences of failure to sustain them. Finally, it requires the application of organization-wide risk analysis to inform decision making and strengthen operations through effective risk management.

b. Occupational Health and Safety Program (OHSP). An official OHSP program will be developed which includes phased implementation for standardized safety surveys and inspections. In addition, an employee training and awareness program will be developed.

3. **Insider Threat Program (ITP) (Continuation from FY17 Plan)**

a. Insider Threat Annual Report (Mandatory). In accordance with program requirements, the first Insider Threat Annual Report will be developed to inform the Board on the status of the program, accomplishments and challenges ahead.

b. ITP Hub Guide (Mandatory). As required by the National Insider Threat Task Force, a Hub Operations Guide (along with other items) is required to achieve full operating capability. Accordingly, OGM will lead the Insider Threat Assessment Team in creating a Hub Operations Guide for identifying, assessing and responding to an insider threat.

c. Insider Threat Expansion (Discretionary). OGM will examine the current Insider Threat Program Directive and Implementation Plan. To that end, we will evaluate the

benefits of expanding the ITP to include insider threats that impact DNFSB's unclassified networks and systems.

4. Physical/Personnel Security (Mandatory)

a. Lenel Security System (Continuation from FY17 Plan). Complete the project to upgrade the Lenel security system and ensure compliance with DOE physical security standards for the Limited Area (LA). Additional upgrades for the Data Center and an annual maintenance contract will also be included.

b. Personnel Security Processing. Develop the infrastructure required to independently process background investigations for DNFSB employees and candidates to initiate and adjudicate Tier 1, 2 and 4 investigations/reinvestigations (HSPD-12 and public trust) with the Office of Personnel Management. This is a no-cost effort to prevent backlogs resulting from outside processing.

5. Information Security (Classified and Unclassified Information) (Mandatory)

a. CUI Implementation. Implement the first phase of the CUI program in accordance with Executive Order 13556, Controlled Unclassified Information and associated implementing directive. This initiative includes development of operating procedures, employee training and awareness and self-assessment standards. The CUI Implementation Plan submitted to NARA specifies implementation in FY 19.

b. OPSEC Program. Develop an implementation plan to stand up an operations security program to protect critical information, both classified and unclassified, to ensure personal safety and successful operations.

c. DOE Security Assessment. Host the DOE information security program assessment and develop a Corrective Action Plan to address findings and recommendations contained in the assessment report.

Information Technology

The Information Technology (IT) submission for the FY18 OGM Work Plan is provided below. While adding ten new major and complex initiatives, FY18 will continue to build on FY17 infrastructure enhancements. Our IT environment will remain a dynamic and changing environment, with a major focus on memorializing IT policies and procedures. Please note that the priority of the below initiatives may necessarily change depending upon the results of the FY17 FISMA Audit.

1. Data Environment (Mandatory):

- a. Strategy: The IT staff will develop a strategy for the data environment. The strategy will be used to guide efforts, listed below, to secure the agency's data and strengthen the agency's capability to aggregate, secure, and mobilize critical management information assets for executive decision-making.
- b. Personal Drives: The IT staff will design and configure access on the network to support personal drives to allow employees to save working files and other documentation on a network folder that is only accessible by an individual employee. This will ensure data redundancy to support disaster recovery and COOP programs.
- c. Data Owner Privileges: The IT staff will work with Office Directors to establish a capability to allow data owners the ability to approve, disapprove and modify permissions to access their respective data.
- d. Cloud Capability¹: The IT staff will engineer and implement a data storage capability in a cloud environment to provide cold storage capability for the agency's infrastructure virtual machine images to support disaster recovery and COOP programs.
- e. Encryption for Data-at-Rest: The agency requires an encryption methodology and execution for securing data-at-rest. Research, acquisition and implementation are required milestones in this fiscal year.

2. Content Management (Necessary for Records Management and FOIA Processing):

- a. File Naming Convention: The IT staff will develop, implement and enforce a file naming convention through the use of standard templates to support the effective use

¹ Although data redundancy is mandatory for COOP and disaster recovery requirements, the agency may choose to place the data in the cloud or in physically-owned servers. OGM is recommending a cloud-based storage capability.

of SharePoint, Electronic Records Management and Correspondence Management System.

- b. Metadata: The IT staff will develop, implement and enforce standards to make the discovery of official records and documents more effective.

3. Projects:

- a. Demilitarized Zone (DMZ) (New): The agency will enhance the cybersecurity posture of its IT enterprise by completing the installation and execution of a DMZ. The DMZ will add another layer in the defense-in-depth strategy to protect and keep Controlled Unclassified Information from adversaries and cyber threats. Initially, it will allow OGC to take advantage of the WestKM, system, but IT will have far greater use going forward to segregate data and secure the network from vulnerabilities.
- b. Correspondence Management System (CMS) (Continuation from FY17 Plan): The agency will design, develop and establish a CMS to support acquisitions, general correspondence and the Board voting process. The folder process may also be incorporated into the CMS, dependent upon Board wishes.
- c. Upgrade SharePoint (Continuation from FY17 Plan): The agency will upgrade the existing SharePoint 2010 on-premises system to SharePoint 2016. The agency will analyze to determine if the capability will remain on-premises or move to the Office365 SharePoint Cloud environment.
- d. VoIP Replacement (Continuation from FY17 Plan): The agency has made the decision to move forward to upgrading their existing VoIP system with a FedRAMP certified system. The new system will replace failing desktop instruments and network switches that are over five years old.
- e. Test Environment (New): The agency requires an infrastructure enhancement to increase its stability and reliability, as well as to provide an enhanced user experience. The team will develop and stand up a test environment which include developing effective test methods that provides the necessary insight to the DNFSB as to potential risks, design flaws, weaknesses and negative impacts of introducing new, or the modification of, existing systems within the GSS (General Support System) infrastructure.

4. Cyber (Mandatory):

The agency's continuous monitoring strategy requires further fortification. We will take on that initiative to strengthen network integrity by introducing two additional Cyber tools in our toolbox containing the following features and functionality: Automated Inventory, Hardware Connection Alerts, Credentialed Vulnerability scans, and SCAP-validated scans.

5. Policy (Mandatory):

The agency's existing IT policies require review with anticipation that the majority will require minor to extensive changes. There are also no policies for several functional disciplines or processes. FY18 will be a focus period of time to address policy compliance requirements.

Human Resources

In FY 2018, DHR will focus on strengthening support for agency employees in the area of performance management. All applicable policies and operating procedures will be updated to meet future needs of the Agency and strengthen the accountability of the General Service, Senior Executive Service, and Excepted Service performance management systems (PMSs). All updates and changes to the three PMSs will be communicated across the agency to help ensure that there is a better understanding of the roles and responsibilities assigned to employees, supervisors, and managers in making the PMs more meaningful and successful. The improvements to the PMSs include timely training sessions for employees, supervisors, and managers throughout the performance cycle and the inclusion of specific (and measurable) performance indicators for meeting all established PMS deadlines in the performance plans of all supervisors and managers. DHR will provide continual communication and deadline reminders throughout the year in support of this effort.

1. To further improve the efficiency and usefulness of performance management programs for all DNFSB employees, DHR will oversee the procurement and expanded implementation of OPM's USAPerformance, an electronic performance management system, to all DNFSB pay systems (DN and GS, in addition to the SES). Implementation includes providing applicable training and technical assistance to employees and supervisors.
2. To further improve the efficiency and usefulness of performance management programs for DN employees, DHR will work with OTD to update the DN performance management system in coordination with moving the DN performance management system to OPM's USAPerformance electronic system at the mid-year review timeframe. Implementation includes a new appraisal plan template, and providing applicable training and technical assistance to employees and supervisors.
3. In support and recognition of the need for leadership development at all levels, DHR will develop a handbook for creating Executive Development Plans (EDPs). The Office of Personnel Management recommends an EDP be a requirement for all Senior Executive Service employees and should outline short-term and long-term developmental activities which will enhance the Executive's performance.
4. Once the Adverse Action and Grievances Directives are approved, DHR will provide training sessions to Board Members, supervisors, and employees on the new policies and processes. The training sessions will include changes from current policies, rights and responsibilities based on position, and information on how to initiate and navigate the processes.

5. To support strengthening employee engagement through timely and appropriate recognition, DHR will provide training sessions to Board Members, supervisors, and employees on the new employee recognition policies and processes. The trainings will include changes from current policies, opportunities to recognize others and responsibilities based on position, as well as how to navigate the new processes (including where forms and instructions can be found). DHR will also issue a new agency Employee Engagement Handbook and offer training to Board members and supervisors.

Budget, Finance, & Acquisitions

In FY 18, OGM plans to look at all aspects of budget, finance, and acquisitions at DNFSB. This includes organization of personnel, use of other Federal agencies for support, and our overall business process.

1. OGM will take a hard look at our use of accounting support from another government agency. To that end, we have already contracted for an accountant who will lay out the end-to-end accounting business process at DNFSB. This will drive potential changes and efficiencies in the future.
2. OGM has proposed the position of Chief Financial Officer (CFO) at DNFSB. This singular official will be properly credentialed and titled and will help drive change in this area. This will also decouple budget and contracting and eliminate any conflicts of interest as a result of the combination of those two functions. However, prior to announcing the position, OGM will take a survey of other small agencies to understand the position description in charge of budget and finance departments to make sure the agency is in line with best practices.
3. The agency will standardize its acquisitions process by incorporating all required steps into the new correspondence management system, creating procedures memorializing those steps and training relevant employees. This is part of the correspondence management initiative referenced in the information technology section above, and is an ongoing initiative from the FY17 Work Plan. Development funds for this initiative were obligated and expended in FY17 pursuant to the previous approval.