United States Department of the Interior

NATIONAL PARK SERVICE
1849 C Street, N.W.
Washington, D.C. 20240

IN REPLY REFER TO:

DIRECTOR'S ORDER #11A: INFORMATION and TECHNOLOGY MANAGEMENT

Approved: _____
Director

Effective Date: APR 4 2005

Sunset Date: This order will remain in effect until revised or terminated

Contents:

1. PURPOSE AND BACKGROUND

Director's Order (DO) #11A identifies and documents the National Park Service (NPS) commitment to accomplish the information management tasks that are required by Federal law and by Department of the Interior (DOI) policies. NPS will adopt this policy to manage its information as a national resource. This DO establishes and defines the practices, standards and procedures for the NPS Information Management and Technology governance structure. DO #11A also outlines the authority, roles and responsibilities of the NPS CIO.

DO #11B: Ensuring Quality of Information Disseminated by the NPS provides policy and procedural guidance on ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by the NPS. DO #11A is also associated with the existing DOs relating to Information and Technology, including DO #19: Records Management and DO #70: Internet and Intranet Publishing.

Applicability. This DO applies to all NPS managers, employees, volunteers, contractors and partners engaged in the management or use of information technology (IT) assets owned or operated by the NPS. The policies, procedures and standards in this DO are to be implemented uniformly throughout the NPS. Deviation from DO #11A is not permitted without the written authorization from the CIO. Regional and associate directors and superintendents/program managers may issue clarifying standards and procedures that are not in conflict with NPS or Departmental policy.

Information as a National Resource. The NPS mission statement drives our use of information.

The National Park Service preserves unimpaired the natural and cultural resources and values of the national park system for the enjoyment, education, and inspiration of this and future generations. The Park Service cooperates with partners to extend the benefits of natural and cultural resource conservation and outdoor recreation throughout this country and the world.

As outlined in NPS Management Policies, information is essential to properly execute the NPS mission. For many, it simply provides the knowledge necessary to make responsible decisions. For others, information about events, people and places identifies where we have been and where we are going as a nation. Some of the information we generate may become a permanent legacy of this Nation's efforts to preserve its natural, cultural, historical and recreational assets. Today the pervasiveness of the Internet gives new meaning and value to information by making it more accessible. Whether information communicates status, condition, performance, budget, or ideas

– it is a resource that must be managed to ensure quality and usefulness. For many, information is the most important resource worked with on a day-to-day basis.

Information Management is the means by which we support the organization's data and learning activities: identifying information needs, acquiring information, organizing and storing information, developing information products and services, distributing information, and using information.

IT is the architecture and technology that supports information management. IT includes any activities relating to computers, equipment, software, firmware, voice communication systems, and similar procedures, services, and other resources. IT represents a significant investment for any organization.

Increasing IT Mandates and Controls. There are numerous changes in Federal IT that mandate better management of IT-related risks. Proficient use of electronic information and IT systems is essential to support critical governmental processes. In addition, the Congress and the Administration are mandating tighter control over information. Tighter controls, in turn, are driven by increasing disclosures of information system disasters, increasing electronic fraud, and concerns about national security. The management of IT-related risks is now being understood as a key part of enterprise governance.

IT practices and information management, to be effective, must be standardized and follow industry "best practices" modified to meet NPS needs and to fit our unique operating environment. In addition, there is a growing body of Federal statutes and regulations that govern the management of IT in the Federal sector with which the NPS must comply. In keeping with the NPS organizational structure, IT resources are highly distributed throughout the organization. However, even a decentralized IT organization must employ a minimal, acceptable level of standardization in order to ensure those systems, networks and other integral parts of the IT environment work in unison.

IT governance is integral to management success by assuring efficient and effective measurable improvements in related enterprise information management. The objectives of IT governance are to ensure that: (1) NPS information assets meet the highest standards of confidentiality, integrity and availability; (2) information is available to NPS managers at all levels to support decision-making process; (3) information is available to NPS employees to enable them to perform their work efficiently and effectively; (4) relevant information pertaining to NPS activities is made available to the public for information, educational and scientific purposes; and (5) NPS works in a seamless manner with its partners using technology to promote and foster a common vision and fulfillment of its legal mandates.

2. AUTHORITY

2.1 Authority to issue this DO is found in 16 U.S.C. §§ 1 through 4 (NPS Organic Act) and in Part 245 of the DOI Manual.

2.2 A Federal mandate and authority to carry out a standardized IT program is found in the Clinger-Cohen Act. In 1996, recognizing the importance of IT for effective government, the Congress and President enacted the Information Technology Management Reform Act and the Federal Acquisition Reform Act. These two Acts together are known as the Clinger-Cohen Act.

2.3 The Clinger-Cohen Act established the requirement for Federal agencies to appoint a CIO for developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture. The Clinger-Cohen Act also requires that agency heads establish a process to select, manage and control their IT investments and emphasizes an integrated framework of technology aimed at efficiently performing the business of the NPS.

2.4 Other requirements of the Clinger-Cohen Act are that all Federal agencies develop a capital asset planning process that includes a committee of key decision makers to determine investments; that Federal agencies establish a detailed inventory of all applications, systems and IT assets; that they establish and maintain enterprise information architecture and perform the proper records management functions in conjunction with IT activities.

2.5 Additional laws, policies and regulations governing the IT practices of the Federal sector include:

- President's Management Agenda
- Government Paperwork Elimination Act
- Government Performance Results Act
- Paperwork Reduction Act
- Computer Security Act
- E-Government Act of 2002
- Privacy Act
- Federal Information Security Management Act
- Electronic Government Act of 2002
- Section 508 of the Rehabilitation Act as amended in 1998
- Executive Order on Computer Software Piracy
- OMB Circular A-130 Management of Federal Information Resources
- OMB Circular A-11 Preparing and Submission of Budget Estimate

- OMB Circular A-16 Coordination of Geographic Information, and Related Spatial Data Activities

- National Institute of Standards and Technology (NIST) Standards for IT security

- Departmental Manual (DM) directives associated with IT

- Federal Records Act (44 USC 3301)

3. RESPONSIBILITIES

3.1 The CIO. Responsibility for oversight of NPS IT governance is delegated to the CIO. The CIO's role is to provide Service-wide strategic direction to our information resource management and (IT) activities. The CIO is responsible for developing mission-oriented policy, procedures and standards, and providing effective review, oversight and inspection of NPS IT and management practices and administration. In addition, the CIO will provide, whenever possible, access to IT industry "best practices" in order to ensure that NPS IT efforts meet the highest possible standards. The CIO reports to the Director through a deputy director and is organizationally equivalent to an associate director.

The CLINGER-COHEN ACT states: "The Chief Information Officer of an executive agency shall be responsible for--

> (1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with chapter 35 of Title 44, United States Code, and the priorities established by the head of the executive agency;
>
> (2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and
>
> (3) Promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency."

The CIO is assigned specific operational duties by the Director, including the management of the NPS's two primary operational IT centers. The CIO is responsible for operationally managing all IT assets and infrastructure components that are contained within these centers.
Finally, the CIO is responsible for other programmatic functions and policy areas as assigned by the Secretary and the Director. This includes all of the traditional IT roles and responsibilities, as well as library management, geographic information systems and radio and voice communications outlined in the Secretarial Order 3244.

(1) technology management (enterprise architecture, capital planning and investment control (CPIC) processes, and information technology acquisition);

(2) security management (system accreditation and certification, access control, and compliance);

(3) information management (records management, Freedom of Information Act, information quality, Privacy Act, and the Government Paperwork Elimination Act); *

(4) telecommunications management (network security and optimization, bill auditing and analysis, radio spectrum management, and wireless communication);

(5) inventory and asset management (tracking and accounting of information resources and equipment);

(6) strategic planning (development and redesign of the organization's IT work processes);

(7) project management (monitoring the project scope, schedule, and budget targets); and

(8) IT career/skills management (developing standards and training requirements for IT professionals).

3.2 The Deputy CIOs for National Information Technology Center (NITC) and National Information Systems Center (NISC) are responsible to the CIO for the development of specific enterprise-wide policies and standards within their specific domains. In addition, as directed the Deputy CIO will directly manage the centers located in WASO and Denver.

(1) The NITC located in the Washington, DC Office is responsible for the topology and technology of the NPS. This includes any activities relating to computers, equipment, firmware and similar procedures, and services. The NITC is responsible for all of the traditional IT roles such as Network Control, Active Directory, Telecommunications, the Wireless Program, Messaging and the Central Help Desk The NITC provides oversight of the NPS voice communication program (local and FTS) and provides operational assistance to the senior managers of NPS located in the Main Interior Building.

(2) The NISC located in Denver, Colorado supports the organization's data and software activities: identifying information needs, acquiring information, organizing and storing information, developing information products and services, distributing information, and using information in the advancement of Information Systems in the NPS. The NISC is responsible for WEB Portal Management, Content Management, NPS System Development and Life Cycle, Application development and support, Image Management, Library, Geographic Information

---

*Information management functions are under the purview of the CIO, as required by Secretarial Order 3244. As provided for in 145 DM 4, the Associate Director for Administration, Business Practices and Workforce Development provides oversight, policy guidance and direction to field units in this functional area, in close cooperation with the CIO.

Systems (GIS), Information System Project Management, Data System and Business architecture.

3.3 The Information Officers (IO) co-exist with the CIO at the regional and associate director level and are designated by the regional/associate directors for the purpose of managing the IT assets directly under their organizational area of responsibility and authority. In addition, each regional/associate director must assign the duties of a technology officer (TO), a security manager and a GIS coordinator to appropriately trained staff. The regional/associate director may determine that the duties of the IO, TO and security manager may be co-located in less than three staff members, but only where the size of the organization is small enough to permit combining duties to less than three separate employees. The CIO will have input into the selection and performance evaluation of IOs as necessary to carry out the mission and goals of DO #11A.

3.4 Regional and Associate Directors are responsible for input, implementation, support, and funding to accomplish or ensuring the following within their area of operation:

(1) NPS IT strategic plan;
(2) NPS components of the Interior Enterprise Architecture
(3) NPS IT Capital Plan and Budget;
(4) IT Security Plans and Continuity of Operation Plans for all systems under their sphere of management;
(5) Compliance with all Federal statutes and regulations governing the management of Federal IT assets;
(6) Conformance with this DO #11A, DOI IT standards and requirements, and all NPS standards and policies.

The IO, TO and Security Manager will provide the necessary guidance to complete the above responsibilities.

3.5 Superintendents, Center Directors and Program Managers are responsible and accountable for the management of IT assets and systems within their respective areas. Each superintendent, center director and program manager is also responsible for overseeing the development of IT assets and systems, ensuring compliance with all Federal IT requirements and for participating in the Service-wide IT governance structure.

Management of the IT infrastructure occurs in the regions, parks and programs. The decentralized nature of the organization requires that the responsibility and authority to carry out various aspects of the IT governance and management processes be delegated to the associate and regional directors. Certain authorities and responsibilities are further delegated to superintendents and program managers who are responsible and accountable for the management of IT assets and systems within their respective areas.

4. CONTROLLING POLICIES

4.1 Executive and Statutory Policies for managing IT assets authorities are listed in section 2 above. New laws and policies are continually enacted in the IT arena and this DO #11A and/or accompanying level 3 responsibilities will be updated as required to reflect necessary changes. However, the absence of a specific law or regulation from the terminology in this DO #11A does not excuse or limit the level of compliance that NPS must legally achieve.

4.2 DOI has published policy and a series of IRM bulletins pertaining to IT and systems that are applicable. In addition, DM 375 19 outlines the IT security responsibilities of DOI bureaus. These directives and standards implement statutory provisions, public law, and regulations relating to IT administration. The NPS will abide by these DOI policies and procedures and implement them through DO #11A.

5. GOVERNANCE STRUCTURE, OPERATIONAL POLICIES, PROCEDURES AND STANDARDS

5.1 Information and Technology Councils and Committees

Managing systems in a decentralized organization requires greater levels of communication than in organizations that are centralized. Information about the cultural and natural resources we manage and influence and about our visitors and the customers we serve represents a resource for the NPS—a resource that we are expected to manage to ensure quality, availability, and security. To meet the needs of the organization and ensure that information is properly managed, several councils and committees are recognized. This DO expressly establishes and/or recognizes the following IT councils and committees within the NPS. The CIO is responsible for ensuring the successful operation of all these committees. These advisory groups exist to provide NPS managers and staff a meaningful opportunity to participate in the formulation and recommendation of Service-wide IT practices, standards, initiatives and plans.

- **Investment Council (ITIC)** – Established to make IT investment recommendations to the Director. Consists of upper-level management and is chaired by the Deputy Director for External Affairs. The Clinger-Cohen Act requires Federal agencies to view their investments in IT as a single portfolio of investments, similar to a portfolio of financial investments. NPS develops capital plans and justifications for all capital asset acquisitions, including major IT systems. The purpose of the ITIC is to review all major IT investments from a business perspective in order to ensure that they meet the mission, goals and objectives of the NPS. The ITIC will provide oversight for project performance by reviewing each IT investment on a quarterly basis to determine if the project is meeting its business, schedule, cost and performance goals. The ITIC will identify appropriate corrective actions for each underperforming project.

- **Information Management Council (IMC)** – Established to provide input on all information management related matters within the NPS. Consists of one representative from each of the regions, associate director, superintendent's, Comptroller's Office and United States Park Police (USPP) organizations and is chaired by a member selected from the Council. The IMC provides recommendations to the ITIC for all major IT investments.

In addition, the IMC reviews standards, manages the IT governance review process, enterprise architecture policies and standards and provides advice and guidance to the CIO as deemed appropriate by the Council.

- **Technology Committee** – Established to address the detailed technical aspects of IT issues. Consists of the TOs from each region, associate director, and USPP organization. The Technology Committee will be intimately involved with the development and implementation of Service-wide IT initiatives relating to technology. The Chief TO chairs this Council and it will meet as necessary to discuss technical and operational issues.

- **Superintendent IT Forum** – Created to provide superintendents with significant input

to the NPS's IT initiatives. Two members from each region (from parks of varying sizes) will meet once a year. The primary purpose of this Forum is for the Office of the CIO (OCIO) to develop a detailed listing of the needs and issues of the superintendents. The Chair for this forum would be selected from the superintendents on the Committee.

- **Geographic Information and related Spatial Data Committee** – Established to represent the NPS GIS community. Chaired by a member selected from the Committee, with representatives from regions, associate directors, superintendents, parks and national program offices such as Fire, Natural Resources, Cultural Resources, Lands, Law Enforcement and Maintenance. The purpose of the GIS Council is to provide strategic leadership for the NPS GIS Program on implementation of GIS, information systems and related technology plans, including direction on policy, program direction, initiatives, funding priorities, and organizational needs. It also provides guidance on appropriate technology, data management, serves as the approving authority for spatial data standards, readily accessible data and applications to fulfill the mission of the NPS.

- **Web Committee** – Established to ensure that all Federal and Departmental Internet standards are being met and to ensure that a common look and approach to web development and content management is implemented throughout the Service. The Web Committee consists of one member from each of the Regions and Associate Directors' offices and a limited number of additional representatives specified in the Web Committee charter.

- **IT Security Committee** – Established to ensure that all IT security issues and challenges are addressed. This Committee is chaired by the NPS IT Security Manager and is comprised of the IT Security Managers selected by regional directors, associate directors, and USPP.

- **Configuration Management Boards (CMB)** – The CIO may create CMBs for general support systems and Service-wide applications as appropriate. The CMBs become an element of the ownership component of that system and members are chosen from the NPS community at-large.

Other temporary working groups and committees may be established by the CIO to address special concerns, initiatives or functions. All such working groups and committees will be cost beneficial and will clearly further the NPS IT goals and objectives.

5.2 Service-wide Operational Policies and Procedures
In order to meet Federal IT requirements and policies, the NPS must establish a number of guiding documents and handbooks that will govern the management and administration of NPS IT assets. The CIO is responsible for the development, implementation and maintenance of these documents. The CIO has the authority to issue bulletins pertaining to IT and systems that are applicable to NPS and are necessary to ensure NPS compliance with the IT requirements of Federal law and DOI policy. All organizational components within the NPS are required to participate and comply with these requirements and the IT documents listed below. The following guidance will be developed and maintained on InsideNPS:

NPS Enterprise Architecture (EA) – An EA is the explicit description and documentation of the current and desired relationships among business and management processes and IT. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the NPS wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes include NPS capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with the Government Paperwork Elimination Act, end user satisfaction, and IT security. The NPS must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and IT, at an appropriate level of detail. NPS implementation of the EA consistent of the following principles:

(i) Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms;

(ii) Meet IT needs through cost effective intra-agency and interagency sharing, before acquiring new IT resources; and

(iii) Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

- **NPS IT Capital Plan and Process** – a detailed five-year view of the NPS anticipated requests for expenditures on IT initiatives and projects.

- **NPS IT Continuity of Operation Plan** – a detailed manual outlining the procedures to follow in case of a disaster, natural or otherwise. Articulates how systems would be brought back on line, what systems would be brought up first and who would be the first users back on line.

- **NPS IT Security Program Plan** – a detailed program and corresponding plan that specifies the minimum risk mitigation requirements of IT resources for which NPS is responsible in the implementation of a secure computing environment.

- **Standards of Behavior for the Security of NPS Information Resources** – establishes

the rules for each NPS user as related to NPS IT assets.

- **NPS IT Strategic Plan** – a detailed five-year view of the NPS key IT initiatives and goals and objectives.

- **NPS System Certification and Accreditation Process** – establishes the process by which NPS major applications and general support systems are certified and accredited to meet the requirements of OMB A-130, Appendix III and conduct periodic reviews.

- **NPS Information Systems Life Cycle (SLC)** – a handbook that outlines the procedures and processes that must be employed, beginning with the development/acquisition of new applications, through the point at which the system is retired and eliminated. Compliance with the SLC must be met by all NPS Service-wide systems, those systems exceeding a specific dollar threshold, systems of special importance (as designated by the CIO), and all financial systems regardless of the cost.

- **NPS Technical Standards Manual** – a detailed manual outlining the minimum standards for NPS hardware and software and the acceptable hardware and software products that may be used in the NPS computing environment.

- **NPS Data Management Manual** – A detailed manual outlining the data management standards.

- **NPS Web Development Standards** – a detailed outline of the acceptable practices and requirements for the development of any web-enabled document that will be made available externally or internally.

- **NPS Section 508 Implementation Plan** – establishes the process for developing, coordinating, and implementing standards and guidelines for the Section 508 of the Rehabilitation Act of 1973.

The manuals, handbooks, and documents listed above will be made official requirements of the NPS through an official review and approval process conducted formally through the IM Council.

5.3 Regional/Associate Operational Policies, Procedures and Plans

The following procedures and plans must be developed at each regional and associate director level where there are sufficient IT assets to warrant their development:

- IT Security Plan for each major application.
- A capital spending plan that outlines IT expenditures for the current and projected next two fiscal years.
- Management Control Reviews conducted at least once every three years, or more often if substantial changes to the system or application are made.

Regional and associate directors may issue additional internal procedures as long as they are consistent with statutory, regulatory, Departmental and NPS requirements.

5.4 Cooperation with the DOI and other DOI Bureaus
The NPS CIO will work closely with the Department OCIO on all Department-wide IT issues. The NPS will make every effort to ensure that its IT infrastructure is compatible with DOI. In addition, the NPS CIO will work with DOI bureaus and other appropriate agencies to find cost-sharing opportunities and to promote inter-operability at the local, regional and national levels wherever possible.

5.5 Development/Acquisition of IT Assets
The development/acquisition of all NPS IT assets must be conducted following the standards and policies outlined in this DO. Personal use systems, such as databases and spreadsheets, that are used to enhance personal productivity, should also be developed using NPS standard software products.

The NPS seeks to establish an integrated, managed IT infrastructure. System development/acquisition activities will be conducted within an organizational framework and will seek to leverage the use of regional and park developed systems at other sites to the greatest extent possible, unless such system is of unique need and design pertaining to a specific organization. Some NPS programs may require special software for sensitive data or protected information resources that should not or cannot be managed by NPS standard software.

The CIO must approve all procurements for IT hardware, software or consulting services that support the management, development or operation of an NPS IT application that exceed $10,000. Purchasing of IT assets will be conducted in the most effective manner possible and will conform to the NPS Standards Manual and Information Architecture. Exceptions may be granted only by the Deputy Director for External Affairs.

5.6 Management of IT Assets
All IT assets must be strictly monitored and accounted for by the system owner using the NPS IT Asset Inventory system located and accessed on InsideNPS. All equipment, systems and personnel must be accurately identified and updated as changes are made.

5.7 IT Security
All IT assets must be maintained in a secure manner, both physically and electronically. All information owners must adhere to the provisions of this DO, DM 375 19 and OMB A-130 Appendix III as well as all other Federal requirements that pertain to the management of Federal data.

All major NPS systems must be properly certified and accredited before they are put into operation. System owners must follow NPS guidance on the certification/accreditation process. NPS systems (such as the Wide Area Network, General Support System, Lotus Notes, Facility Management Software System (FMSS), Incident Management and Reporting System (IMARS), and My Learning Manager) may not be officially used until they have been properly certified and accredited by the Director in accordance with DM 375 19.

Networked systems will maintain access control mechanisms consistent with DOI, NPS guidelines and system owners will ensure compliance with all requirements.

5.8 Data Integrity Standards

All information owners will maintain all official NPS records and data in a manner which meets the highest data integrity standards, including timeliness, accuracy and completeness (also see DO #19). Each information owner will take whatever steps necessary to ensure that NPS systems have sufficient data quality reviews and audits from both an internal system perspective, as well as externally through control reviews.

All NPS data systems will develop data dictionaries and conform to available NPS organization-wide dictionaries.

Geographic Information and Metadata must meet all Federal standards, DOI standards and NPS standards.

5.9 IT Investment Process

The Clinger-Cohen Act and OMB Circular A-130 direct Federal agencies to use a comprehensive capital planning process for selecting and managing IT investments. To this end, NPS established the IT Investment Council and the NPS IT Capital Planning and Investment Process whose objective is to incorporate IT capital planning processes into the business practices of NPS, and ensure investments align with the NPS mission while minimizing risks and maximizing returns throughout the investment's life cycle. This evolving process, guided by the EA, provides an analytical framework for linking IT investment decisions to strategic objectives, mission achievement, and business plans. IT capital assets are managed throughout all phases of their life cycle. The project manager and the project management team develop and accomplish project milestones within the expected cost parameters established by the business case and cost benefit analysis. All NPS IT investments are subject to review and approval by the ITIC. However, the level of review will be commensurate with the size and importance of the investment.

Major acquisitions, projects, applications or systems must prepare Capital Asset Plans, (Exhibit 300s), identify the full cost of each project through its entire life cycle. The Capital Asset Plan will contain a thorough analysis of all viable alternatives, including consideration of outsourcing to other agencies or the private sector. The Capital Asset Plan contains a cost benefit analysis, risk assessment, alternatives analysis and performance measures to aid management in determining if a proposed investment should go forward. Major investment plans must be submitted to the Department and to OMB.

OMB defines major systems as IT acquisitions, projects, or applications, with a total life cycle cost of $35 million dollars or more. Other systems with life cycle costs below this threshold will be designated as major based on their high visibility, high risk, or special importance as determined by the NPS CIO or higher authority.

Non-major investments must document their projects through the Exhibit 300-1, a shorter plan that identifies the project budget, schedule, goals and objectives. All investments, major and non-major, will be documented in the NPS System Inventory and conform to NPS Application

Enclave requirements. Capital Asset Exhibit 300s or 300-1s must be developed and updated quarterly. The quarterly report will present the projects progress relative to the initial costs, schedule, and performance goals as well as present updated earned value statistics.

The NPS has established a two-pronged approach for the evaluation and review of IT investments. Under this approach the CIO will get input from the IM Council, System Owner, Technology Committee, Data Management Committee, and EA. The CIO will present the resulting analysis to the ITIC for consideration in their evaluation of proposed investments. ITIC approved investments are submitted to Project Management Information Systems/Operations Formulation System (PMIS/OFS) and follow all budgetary processes and requirements.

The OCIO will establish a yearly schedule for the submission of Exhibits 300 and 300-1. The OCIO will provide a format for system owners/project mangers to use in submitting quarterly briefings to the ITIC for their review. When problems are identified, the ITIC will recommend appropriate corrective action.

5.10 Human Resources and Training

The CIO will work with NPS leadership to develop a continuous and comprehensive program for hiring, training and retaining competent IT professionals throughout the NPS. Assistance available through this program will include the development of specific training courses, position descriptions, access to cost-effective training opportunities, and establishment of certification requirements within NPS for various critical IT positions.

5.11 OCIO Policy

In order to keep our IT program current, the CIO will develop and issue mandatory and high priority OCIO Policy that summarize and outline the policies and procedures relating to constantly changing non-discretionary statutory, regulatory or OMB directed information management and technology requirements. In particular, the security of IT systems is an area of concern that requires immediate and ongoing attention.

5.12 Compliance

Compliance with the requirements of DO #11A is an integral component of IT governance. The CIO will provide oversight and review of all IT operations within the NPS. The CIO is required to take all steps necessary to mitigate non-compliant incidents with the responsible organization. However, if compliance is not attained, or not likely to be attained, the CIO will notify the Director and the Deputy Director for External Affairs and recommend appropriate action.

Organizations having processes, policies, software, hardware, etc. that are not in compliance with the requirements and standards of DO #11A at the time of its publication must request a temporary waiver of the requirement through the CIO and specify resources needed and a target date to comply. The staff of the CIO can assist in developing a compliance plan.

---------- *End of Director's Order* ---------