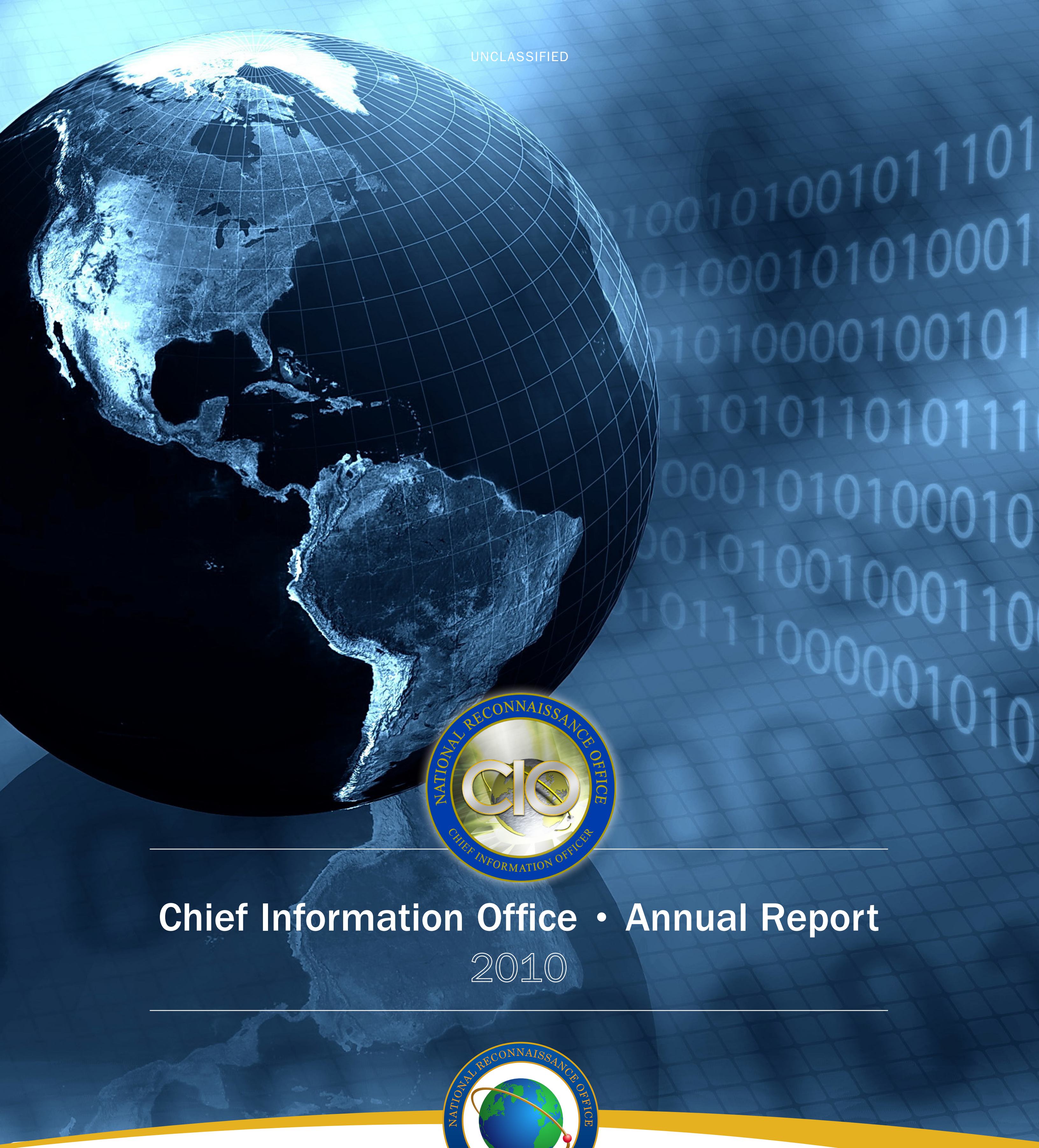


Chief Information Office • Annual Report

2010

NATIONAL RECONNAISSANCE OFFICE

Letter from the Chief Information Officer

It is my pleasure to provide you with the 2010 National Reconnaissance Office (NRO) Chief Information Office (CIO) Annual Report. Throughout the year, the CIO has worked to put in place a solid foundation for enterprise management of information technology (IT), information assurance (IA), and information management (IM) at NRO. This report highlights key initiatives that contributed to building that base.

Please join me in celebrating the CIO's accomplishments for 2010. We made great progress in the areas of IT Governance, IT Architecture & Strategy, Information Assurance, IT Investment Management, IT Workforce Development, Spectrum, and Innovation. CIO staff represented NRO in Intelligence Community (IC) and Department of Defense (DoD) forums, supporting many initiatives geared toward increasing information sharing and achieving IT efficiencies.

I would like to extend my appreciation to the many partners and stakeholders within the NRO, IC, and DoD who contributed to the CIO's successes during 2010. The support of these stakeholders is critical to advancing the role that IT plays in support of the NRO vision of *Vigilance from Above*.

Jill T. Singer

Jill T. Singer
Chief Information Officer

Table of Contents

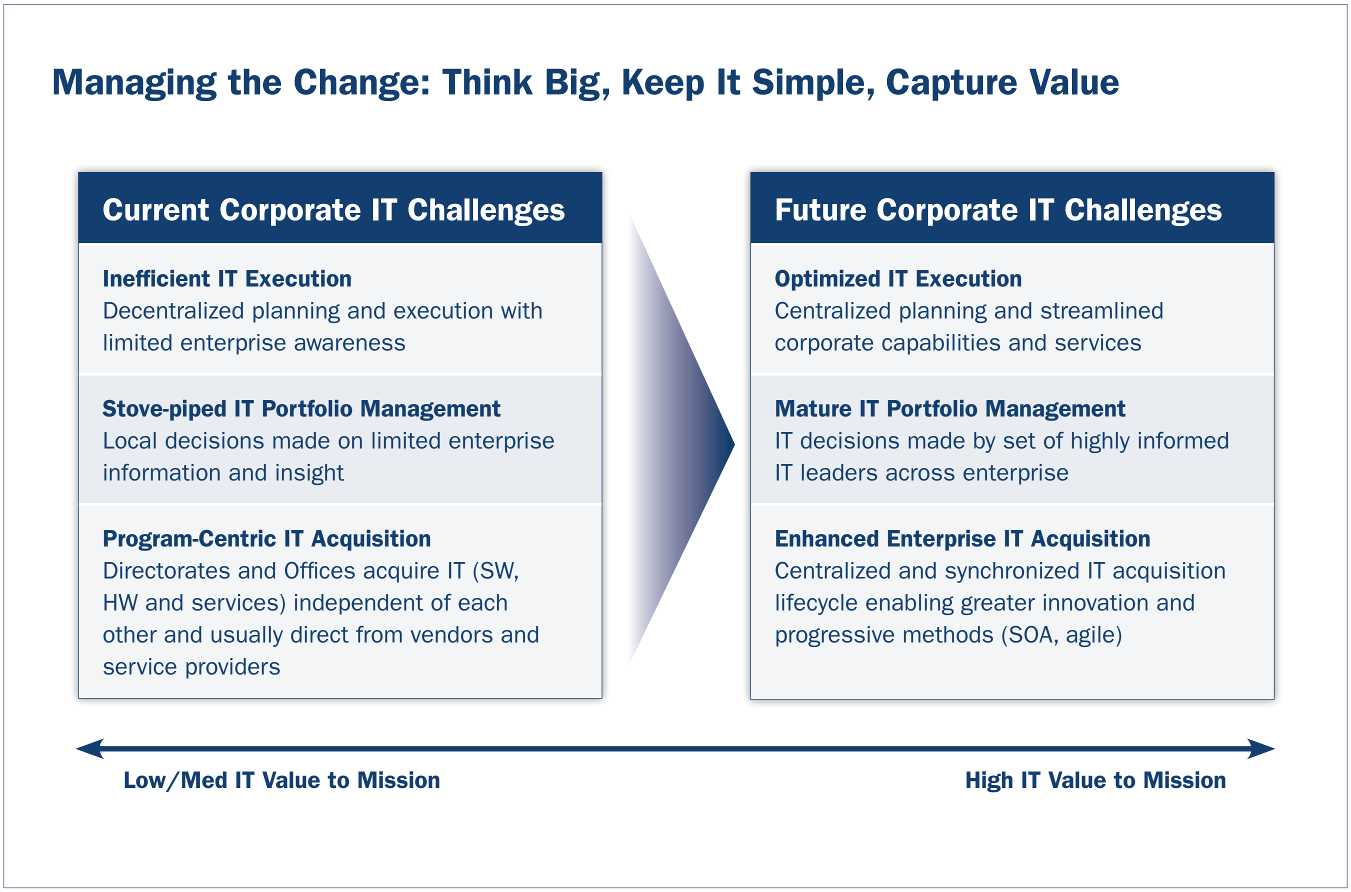
Introduction

Over the past year, the National Reconnaissance Office (NRO) Chief Information Office (CIO) has worked to increase the value that information technology (IT), information assurance (IA), and information management (IM) provide to the overhead reconnaissance mission.

The CIO has articulated a future state in which IT support to the NRO mission is optimized. This future state aims to maximize IT effectiveness and efficiency, and reduce the time to market for IT solutions. The NRO will manage IT corporately, rather than within stovepipes.

Realizing this vision will require collaboration, participation, and support of key stakeholders throughout the NRO, the Intelligence Community (IC), and Department of Defense (DoD). The CIO focused this year on building and strengthening those partnerships. CIO leaders and staff led and participated in cross-organizational working groups and partnership meetings aimed at improving Information technology, information assurance, and information management (IT-IA-IM) throughout the NRO. Associate Chief Information Officers (ACIOs) within each Directorate and Office (D and O) acted as critical liaisons between the CIO and the rest of NRO. The achievements outlined in this report are the direct result of the relationships between the CIO and its partners.

This 2010 CIO Annual Report focuses on the CIO's accomplishments and positive impact within the NRO, IC, and DoD. The report concludes with a look ahead toward 2011 as the CIO, in partnership with the NRO Ds and Os, endeavors to strengthen IT contributions to the NRO mission.



Managing the Change: Think Big, Keep It Simple, Capture Value

Current Corporate IT Challenges

Inefficient IT Execution
Decentralized planning and execution with limited enterprise awareness

Stove-piped IT Portfolio Management
Local decisions made on limited enterprise information and insight

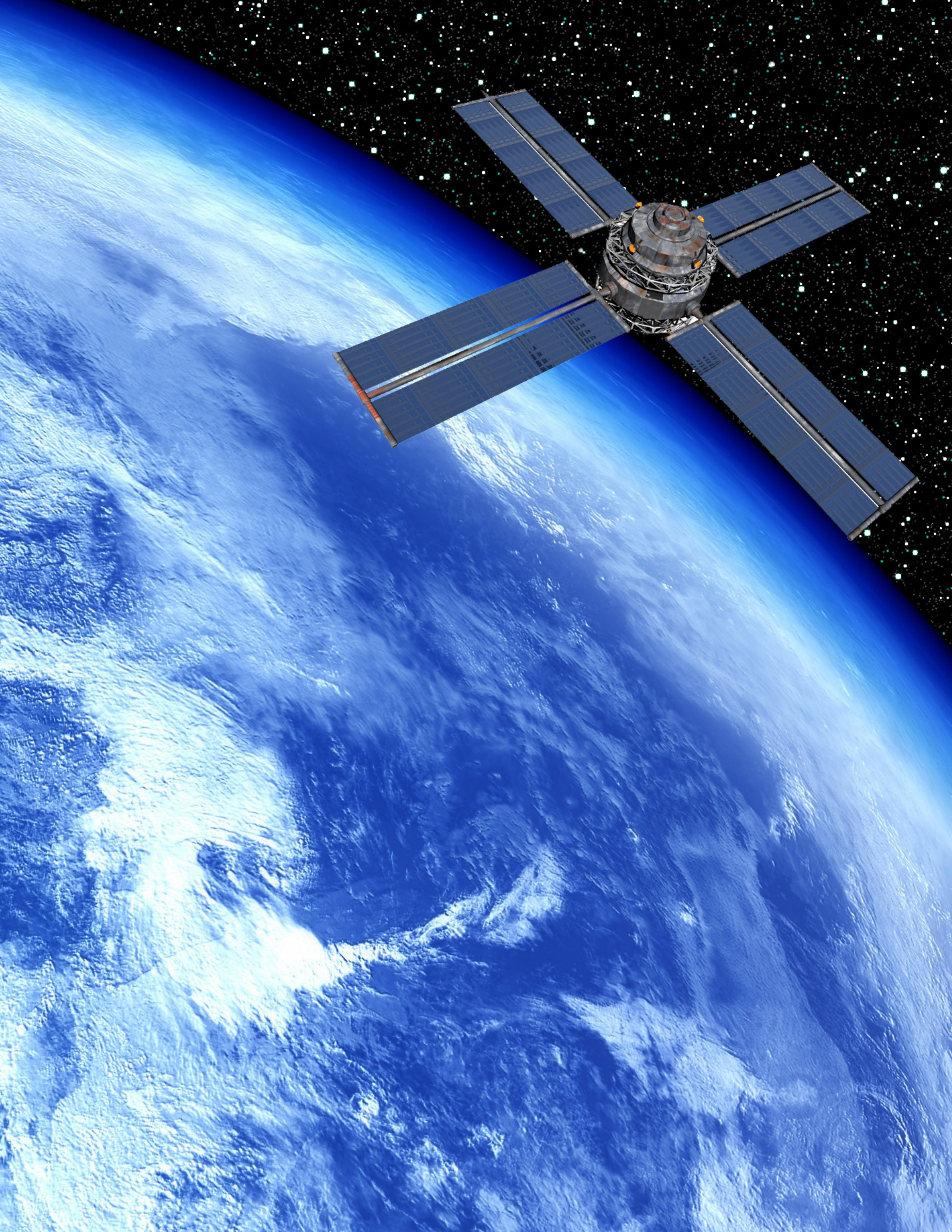
Program-Centric IT Acquisition
Directorates and Offices acquire IT (SW, HW and services) independent of each other and usually direct from vendors and service providers

Future Corporate IT Challenges

Optimized IT Execution
Centralized planning and streamlined corporate capabilities and services

Mature IT Portfolio Management
IT decisions made by set of highly informed IT leaders across enterprise

Enhanced Enterprise IT Acquisition
Centralized and synchronized IT acquisition lifecycle enabling greater innovation and progressive methods (SOA, agile)



2010 Major Accomplishments

IT Governance

The CIO made significant progress toward enabling enterprise management of NRO IT through implementing forums, policies, and instructions. Throughout the year, CIO partnered with NRO subject matter experts and stakeholders to develop, coordinate, and publish IT-IA-IM policies and governance processes.

IT Executive Committee

In June 2010, with approval from the Director, NRO (DNRO), the Chief Information Officer established the Information Technology Executive Committee (ITEC) to direct IT-IA-IM strategic planning, architecture transition, and investment priorities.

The ITEC specifically focuses on the following:

- **Strategic Decisions:** Approval of IT-IA-IM strategies, architectures, architecture transition plans, and investment plans;
- **Resolution of Systemic Issues:** Establishment and oversight of working groups to resolve high-impact, cross-NRO IT-IA-IM issues; and
- **High Profile Activities:** Review, endorsement, and promotion of IT-IA-IM projects/programs.

The ITEC is the first step towards establishing enterprise-level governance of IT. It does not replace D and O decision-making structures, authorities, or accountability, and does not function as a program/project or service control gate. Though still new, the ITEC has already made important decisions, including approving the IT Target Architecture (ITA) Description, IA Domain Architecture Description, and the IA Domain Technical Roadmap.

The ITEC selected high profile activities to be tracked during Fiscal Year (FY) 2011, and is already receiving initial briefings. These projects and programs deliver important common services and infrastructure elements to the NRO, DoD, and IC, ushering in the future of NRO IT, and laying the foundation necessary to understand and overcome the ever-evolving cyber threat. Finally, the ITEC chartered two working groups to address long-standing, systemic issues; IT procurement and IT requirements.

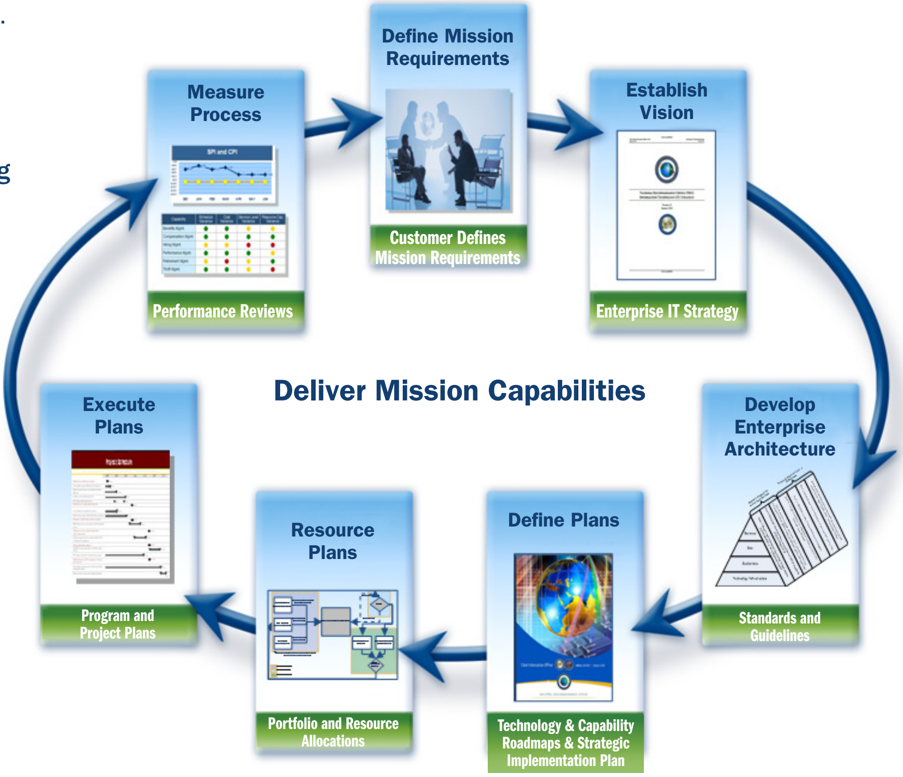

Define Mission Requirements
Customer Defines Mission Requirements
Establish Vision
Enterprise IT Strategy
Develop Enterprise Architecture
Standards and Guidelines
Define Plans
Technology & Capability Roadmaps & Strategic Implementation Plan
Resource Plans
Portfolio and Resource Allocations
Execute Plans
Program and Project Plans
Measure Process
SPI and CPI
Performance Reviews
Deliver Mission Capabilities

Figure 1:
The ITEC aims to mature the IT planning process at NRO.

2010 Major Accomplishments (continued)

High Impact IT-IA-IM Policies

The CIO led the development of many high impact policies during 2010. Most recently, the CIO fostered collaboration across the NRO to produce a high interest policy on Portable Electronic Device (PED) Authorization and Use. In response to Inspector General recommendations, the CIO worked collaboratively with the NRO Ds and Os to analyze report findings and develop a comprehensive policy for the NRO that addresses both government- and personally-owned PEDs. Signed by the DNRO on 29 November, this policy consolidates previous guidance into a single document. The policy provides guidance on the use of PEDs that aims to balance employees' desire to bring portable technology into the workplace with the need to maintain a secure and reliable environment. In 2011, the CIO will work with the Ds and Os to develop the guidance and processes necessary for implementing the new PED policy.

The CIO also produced three new policies providing firm guidance on the issuance and management of accounts on the NRO Management Information System (NMIS), the Secret Collateral Management Information System, and the Unclassified Management Information System. These policies standardized account approval processes in response to management concerns regarding access to NRO information systems. By standardizing these processes, CIO laid the foundation for future automation of account approvals and improving the IA posture through annual account review.

Another area in which the CIO provided overarching policy guidance was the establishment of an IC Display Name convention for the NRO Contractor Wide Area Network and any NRO networks with foreign national participation (referred to as "REL TO" networks) , such as the Integrated Mission Information System. These naming conventions establish a consistent format for each of the directories that provide source data to the NRO Global Address List. The IC Domain Name System policy supports IC Information Sharing initiatives and the DoD strategic intent to unify the Defense Intelligence infrastructure.

Clean Audit

The NRO Office of Inspector General (OIG) contracted with the independent public accounting firm of PricewaterhouseCoopers (PwC) to provide an independent audit of NRO financial statements for the year ended 30 September 2010. The audit examined two aspects of NRO's financial systems: the integrity of NRO financial business processes and the integrity and security of NRO's financial IT systems. The CIO's role in the audit concerned the IT systems and focused on ensuring cooperation among the various service providers involved in supporting the financial IT systems and responding to queries about the information security aspects of the audit. On an ongoing basis the CIO staff and ACIOs ensure resolution of audit findings prior to the next annual audit.

The OIG published the final results in a memorandum to the DNRO, dated 12 November 2010, in which PwC issued an unqualified opinion on the NRO FY 2010 Financial Statements. The NRO is the only IC entity having received an unqualified audit opinion for two successive years, thus establishing the NRO as a leader in business systems, process definition, and IT with the quality and sustainability to ensure the financial statements are fairly presented in accordance with generally accepted accounting principles.

Major System Acquisition

This past year, CIO supported Ground Enterprise Directorate (GED) as it continued to drive to an integrated ground concept. The NRO Ground Enterprise (NGE) consists of four independent but tightly integrated Major Systems

2010 Major Accomplishments (continued)

Acquisitions (MSAs): Command and Control, Mission Management, Mission Processing, and Mission Framework. The CIO acquisition team provided the NGE acquisition Core Team with leadership, direction, and consultation regarding the relatively new MSA requirements (Clinger-Cohen Act Compliance, Information Support Plan, and Intelligence Community Enterprise Architecture Compliance).

After reviewing GED's acquisition documentation and creating an assessment report, the CIO determined that the program demonstrated adequate due diligence with regards to their programmatic documentation and plans, which resulted in certifying compliance and CIO endorsement for these acquisitions. The CIO then championed, liaised, and provided critical external strategic communications between Office of the Director of National Intelligence (ODNI) and DoD acquisition offices and the NGE program manager. Additionally, for the first time, the CIO engaged and supported the Independent Program Assessment (IPA) as an integral team member in the review.

IT Architecture and Planning

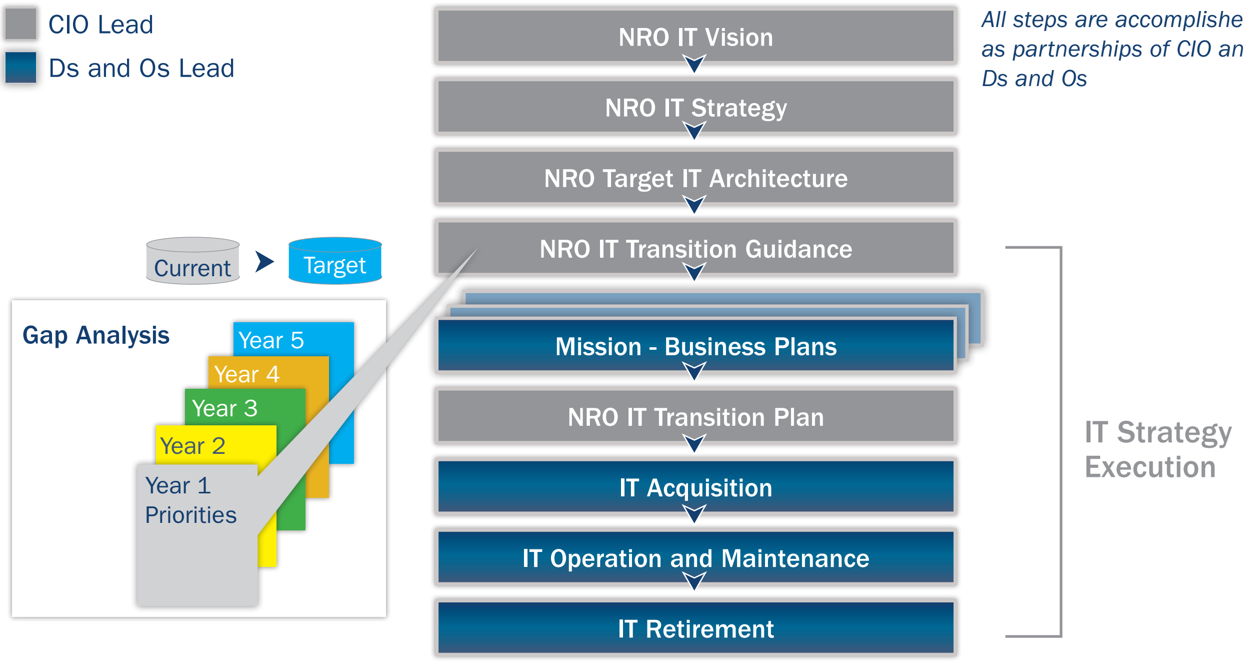
The CIO published several key architecture and strategy documents, provided important guidance to the Ds and Os, and participated in key acquisition activities this year to shape NRO IT.

NRO Information Technology Strategy

The NRO IT Strategy (ITS), developed in coordination with stakeholders across NRO, articulates NRO's IT vision, goals, and objectives, and defines an NRO IT Strategic Planning Process that establishes a direct connection between IT infrastructure and mission. The NRO Corporate Council approved the ITS in January 2010.

The NRO IT Strategic Planning Process identified the need for three additional strategic products; the NRO IT Target Architecture Description (ITA), the NRO IT Transition Guidance (ITTG), and the NRO IT Transition Plan (ITTP); to further focus the IT infrastructure in support of intelligence mission needs.

Figure 2:
IT Strategic Planning Product Lifecycle



All steps are accomplished as partnerships of CIO and Ds and Os

2010 Major Accomplishments (continued)

Since the approval of the NRO ITS, the CIO has completed the ITA and secured its approval by the ITEC. The CIO also drafted the other two strategic products, the NRO ITTG and the NRO ITTP. Additionally, CIO used the ITS to drive the development of the IA Domain Technical Roadmap and the IA Domain Architecture Description.

The ITS has been used as an input to several strategic mission documents, including Systems Engineering Directorate's (SED) NRO Enterprise Plan v 1.0.

NRO IT Architecture

The NRO ITA establishes a common IT target state equipped with IT capabilities to prioritize and drive all future NRO IT investments. CIO led the development of the document and created the content in partnership with several NRO Ds and Os. ITA is the first NRO IT Architecture document that establishes a foundation for IT across the NRO and among NRO partners.

IA Domain Architecture

A key segment of the NRO IT Architecture, the IA Domain Architecture establishes a capabilities framework that enables assured information with the IC and the DoD. The CIO delivered several IA architectural products over this past year that align with the NRO IT Architecture and establish the foundation for a comprehensive IA Architecture. The IA Domain Architecture Description and IA Domain Technical Roadmap identify and organize the NRO IA Architecture components and goals; the IA Domain Technical Architecture Topology provides a visualization of IA capabilities, services, relationships and functions; technical targets articulate specific envisioned end states and identify tasks for Ds and Os to deliver IA capabilities and services in support of the NRO IT Architecture. The ITEC approved the IA Domain Architecture Description and IA Domain Technical Roadmap in November.

UNCLASSIFIED

INFORMATION TECHNOLOGY TARGET ARCHITECTURE DESCRIPTION

NATIONAL RECONNAISSANCE OFFICE

June 2010

UNCLASSIFIED

IA Standards Document

Through collective teamwork, CIO continued to evolve the processes for the NRO Corporate Standards Baseline and the NRO Standards Management Group. During 2010, SED, in collaboration with the CIO, began implementation of the newly published Committee on National Security Systems Instruction (CNSSI) 1253 security controls to the NRO. In doing so, the Information Assurance Standards Document (IASD) was revised and baselined by SED requirements and configuration management boards. The IASD has been baselined in NRO's Enterprise Requirements, Standards, and Best Practices Repository as the corporate standard for NRO's minimum security controls reflecting NRO implementation of the CNSSI 1253, Security Categorization and Control Selection for National Security Systems. This document standardizes IA requirements for all NRO acquisitions and removes previous program management confusion on how or which IA requirements to apply. Two MSAs within GED have required the use of the IASD as the basis for all IA requirements to jumpstart the use of these requirements within the NRO.

IT Service Definition

The CIO initiated the NRO IT Service Definition project in May to identify the IT services provided at the NRO and to assign specific Ds and Os as enterprise-wide providers for each of those services. Through a coordinated effort, CIO, Communications Systems Directorate (COMM), MOD, Management Services and Operations Directorate (MS&O), Business Plans and Operations (BPO), SED, and GED

2010 Major Accomplishments (continued)

established a common taxonomy and framework for the initial identification and definition of NRO IT Services. Business functions, capabilities, stakeholder organizations, and a lead organization were defined for each IT Service Category. The goal of this effort is to eliminate duplication, reduce overlaps, and deliver greater efficiencies and economies of scale to enterprise IT management. Consolidating and managing IT solutions as services, consolidating the number of IT provider organizations, delivering improved performance to its users, and delivering improved cost efficiencies will result in optimized IT services for NRO.

A second area of focus was on defining the IT Service Management process to be used for governing NRO IT Service Catalog, including ordering, approving, and fulfilling IT service requests. IT Service Management processes will enter formal Corporate Business Process Instruction (CBPI) coordination in 2011, along with a joint effort to automate the NRO IT Service Catalog.

IT Investment Management

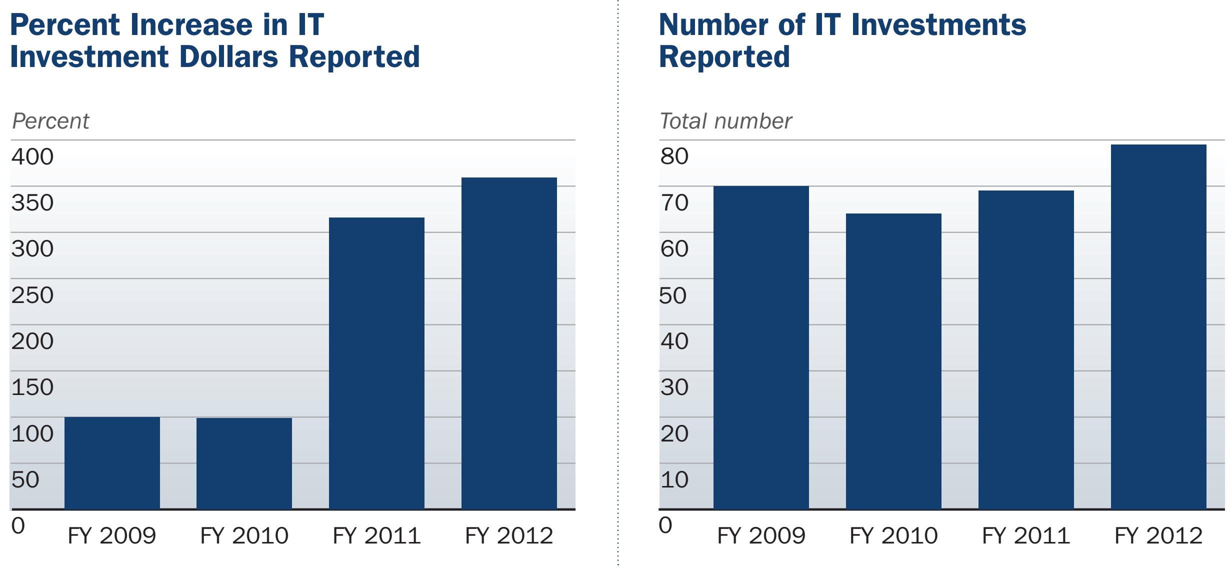
CIO's role in IT investment management within NRO is increasing. In addition to serving as the focal point for investment reporting to Office of Management and Budget (OMB) and ODNI, CIO also provides guidance to NRO organizations concerning their IT investments. IT Investment Management plays a critical role in aligning current and future IT needs to the mission and the CIO ensures consistency between mission goals and the execution of funding.

Exhibit 53/300 Submission

NRO submitted its yearly Agency Information Technology Investment Portfolio Exhibit 53a and Capital Asset Plan and Business Case Summary Exhibit 300 reports to the ODNI in August. This year the CIO also responded to OMB's new requirement to report IT security costs through the Agency Information Security Costs Exhibit 53b. The Exhibit 53b required each agency to identify IT security costs spent in categories such as Manpower and Staffing, IT Security Tools, FISMA Testing, and C&A.

One of the CIO's top priorities is to protect NRO IT investment dollars reported in Exhibits 53 and 300. This year the NRO reported 10 new investments accounting for a 9% increase in dollars over last year's submission, and a 359% increase over 2009. This data serves as a foundation for the CIO to

Figure 3:
Exhibit 53 IT Reporting



Percent Increase in IT Investment Dollars Reported

Number of IT Investments Reported

2010 Major Accomplishments (continued)

understand how NRO IT investment dollars are programmed, budgeted and executed. The information is also used to identify where the NRO can potentially gain efficiencies, absorb cuts and identify trade space. The CIO will continue to work with BPO and other Ds and Os to improve accuracy of reporting and decrease the effort required to develop Exhibits 53 and 300 investment reports.

Technical Planning Guidance

In February, the CIO was asked for the first time by BPO to provide the CIO's priorities and content for the FY 2012 – FY 2017 Program Plan. Despite a tight deadline the CIO was able to submit the five CIO Priorities, which were published in the Technical Planning Guidance. The five priorities support the NRO mission by defining CIO's areas of focus to improve the efficiency and performance of NRO IT systems and business processes. The five priorities are:

- Information Assurance;
- Information Sharing and Collaboration;
- Enterprise Efficiency;
- Effective Management of IT; and
- Frequency Management.

The CIO then developed and presented its program review to BPO. This briefing explained the current state of NRO IT, the issues and challenges facing the NRO, and how the CIO's priorities focus on foundational activities that support a corporately-managed approach to addressing these issues. Throughout the year the CIO championed existing IT programs, projects, and initiatives that support the five CIO Priority areas. The office actively collected data across the Ds and Os on how the programs, projects, and initiatives aligned to the IT Strategy, the IT Architecture, and the goals of the NRO IT community. This information further shapes the IT baseline and prepares the CIO to respond to the FY 2013 – FY 2017 Planning Guidance.

Information Assurance and Cyber Security

During 2010, the CIO continued to forge relationships with the Ds and Os across the organization in order to bring IA to the forefront. Partnership is vital to the success of NRO's IA program. Our accomplishments this year further the cause for developing and realizing a robust corporate-wide IA program to reduce our cyber security risks and enhance our ability to manage and react to cyber events.

Enterprise Information Assurance Program

During the last year, CIO engaged the Ds and Os in substantial planning to further scope and refine the Enterprise Information Assurance Program (EIAP) and its twenty IA Initiatives. The CIO laid the foundational elements of the program with respect to reporting and monitoring for the EIAP. Decisions concerning IA are made through the NRO's established Corporate Governance structure and the ITEC. To govern and oversee the initiatives, the IA Working Groups (Programmatic and Technical) were chartered to assess operational impacts and issues relative to the planning, execution, and operations of these initiatives. Ds and Os actively participated in developing specific IA budget inputs for the first time in the NRO budget acquisition cycle and supported the CIO with defining an IA budget structure that will capture NRO IA expenditures in the future. This budget structure is expected to be implemented in FY 2012 and FY 2013 by the Ds and Os in coordination with BPO.

Certification and Accreditation Transition

The CIO worked this year to refine the NRO's C&A process to align with IC Directive (ICD) 503: IC Information Technology Systems Security Risk Management, Certification and Accreditation and its related guidance. To make the C&A process documentation more readable and implementable, the C&A CBPI was restructured to reflect the Risk Management Framework called for in Committee on National Security Systems Policy 22, ICD 503, and National Institute of Standards and Technology 800-37.

The NRO is now actively implementing the provisions of ICD 503. All Approvals to Operate (ATO) are now made by the CIO. OS&CI is designated as the Certification Agent. All ATOs are required to include a Plan of Action and Milestones for identified liens.

Throughout 2010, NRO has achieved and maintained a 96% accreditation rate of its IT systems and is working to improve upon that score during the next year as the NRO implements continuous monitoring functions.

The ACIO for SED worked very closely with the CIO to ensure that IA, and specifically C&A activities, are addressed in each SED-developed CBPI to further solidify the integration of IA into the systems development, acquisition, and launch/initialization-readiness lifecycles.

2010 Major Accomplishments (continued)

Vulnerability Management

The CIO has been very active in several key Vulnerability Management activities over the course of this past year. Specifically, CIO engaged with Ds and Os across the organization to establish and implement the Enterprise Vulnerability Assessment and Remediation (EVAR) process. Each D and O has a Vulnerability Assessment and Remediation (VAR) team that reports findings and remediation recommendations to the Vulnerability Management Working Group (VMWG), co-chaired by CIO and OS&CI.

The EVAR has teamed with the MOD VAR team to promulgate best practices across the NRO. Quarterly remediation status reports are provided by each D and O to the VMWG and DNRO providing a holistic view of remediation progress and situational awareness enabling the organization's remediation efforts to be more than six months ahead of last year's schedule. This approach significantly improved the NRO's security posture. The EVAR team is currently developing a remediation dashboard for the DNRO and NRO senior leadership to improve IA situational awareness.

Command Cyber Readiness Inspection

The Defense Information Systems Agency (DISA) conducted a Command Cyber Readiness Inspection (CCRI) of NRO's Non-classified Internet Protocol Routing Network (NIPRNet) and Secret Internet Protocol Routing Network (SIPRNet) connections. The NRO received an overall OUTSTANDING rating based on a 94.7% rating for the assessed NIPRNet and 91% for the assessed SIPRNet. The DISA Field Security Operations team concluded that the risk of NRO systems connectivity to the DISA Global Information Grid is considered low due to sound perimeter security and a determined staff working continually to identify areas for improvement. As a result of this activity, key information and lessons were brought back to the organization and findings were communicated and remediated through a joint effort involving COMM, MOD, OS&CI, and Mission Support Directorate (MSD). Looking ahead, the NRO can garner continued success and increase its scores by continuing the partnership established during this inspection and working collectively towards closure of the findings documented.

National Cybersecurity Awareness Month

The CIO and OS&CI partnered to sponsor a variety of cyber security awareness events throughout the month of October 2010. Subject matter experts from federal government, industry, and academia presented on new and evolving cyber threats and computer network defense approaches, and senior government and DoD strategists spoke on the way ahead for cyber security. In addition to the speaking events, a technology expo provided security vendors the opportunity to share their products in support of the President's 2010 National Cybersecurity Awareness Month.

OCTOBER 2010
NATIONAL
CYBERSECURITY
AWARENESS MONTH
StaySafeOnline.org

Figure 4: NRO Chief Information Officer Ms. Jill T. Singer kicks off the speaking events for Cybersecurity Awareness Month.

Figure 5: The Honorable Howard Schmidt, White House Cyber Security Coordinator, addresses the JD Hill Auditorium.

2010 Major Accomplishments (continued)

Annual Security Awareness Refresher Training

During 2010, 94% of the NRO population completed the annual security awareness refresher training required by both the Federal Information Security Management Act (FISMA) and DoD Directive 8570. The CIO worked with Office of Security and Counterintelligence (OS&CI) to track and report completion of the training course and to attain compliance with the Intelligence Community Public Key Infrastructure (PKI) mandate. After the training deadline passed, Mission Operations Directorate (MOD)/Network Operations Group deactivated the NMIS accounts of personnel who did not complete the training course. Additionally, by PKI-enabling the database that hosted the training, the NRO issued IC PKI certificates to 98% of its user base. These actions yielded three benefits: NRO's compliance with FISMA and DoD 8570 requirements remained high, NRO was able to meet a long-standing PKI mandate, and the NRO was able to delete a number of unused NMIS accounts.

Cross Domain Support Office

The CIO formally established and staffed the Cross Domain Support Office (CDSO) in May 2010. The CDSO team is building a collaborative community within the NRO to better understand mission requirements with the goal of providing value-added cross domain solutions (CDS) to protect NRO's information and enable a secure mission environment. Additionally, the team is reaching across the DoD and IC to better identify common new development efforts and opportunities for CDS reuse. The CDSO has established an internal portal to better disseminate product information to various system and program offices. The CDSO is currently supporting the joint GED and MSD study of deploying virtualized CDS to reduce the overall cost to procure and operate CDS.

IT Workforce

This year the CIO championed two key activities for the development of the IT workforce at NRO. Improving compliance with DoD Directive 8570, which requires training and certification of information assurance personnel is one key activity. The second is the creation of an NRO-wide IT workforce council. In addition to these activities, the CIO partnered with the Office of Strategic Human Capital (OSHC) to address the need to fill mission critical IT positions by implementing strategic initiatives to attract employees with key IT skills to the NRO.

IT Workforce Council

Chartered in May, the IT Workforce Council is the first organization created within the NRO specifically for our IT employees. Jointly sponsored by the CIO and the Director of OSHC, the IT Workforce Council identifies IT workforce issues, crafts recommendations, and proposes high-impact initiatives to NRO senior leadership. The Council's 27 members span the NRO – representing each of the parent organizations, NRO IT occupations, and NRO Ds and Os.

In 2010, the IT Workforce Council embarked on two initiatives to build an IT workforce community at NRO. The first was to establish an information sharing venue for NRO IT employees with outreach to the IC. The second initiative will develop career development and training resource roadmaps for NRO IT employees. The IT Workforce Council will engage stakeholders from OSHC, the NRO Unity Council, and NRO parent IT organizations to address many of the factors the IT Workforce Council identified as significant to enhancing the NRO experience for IT employees.

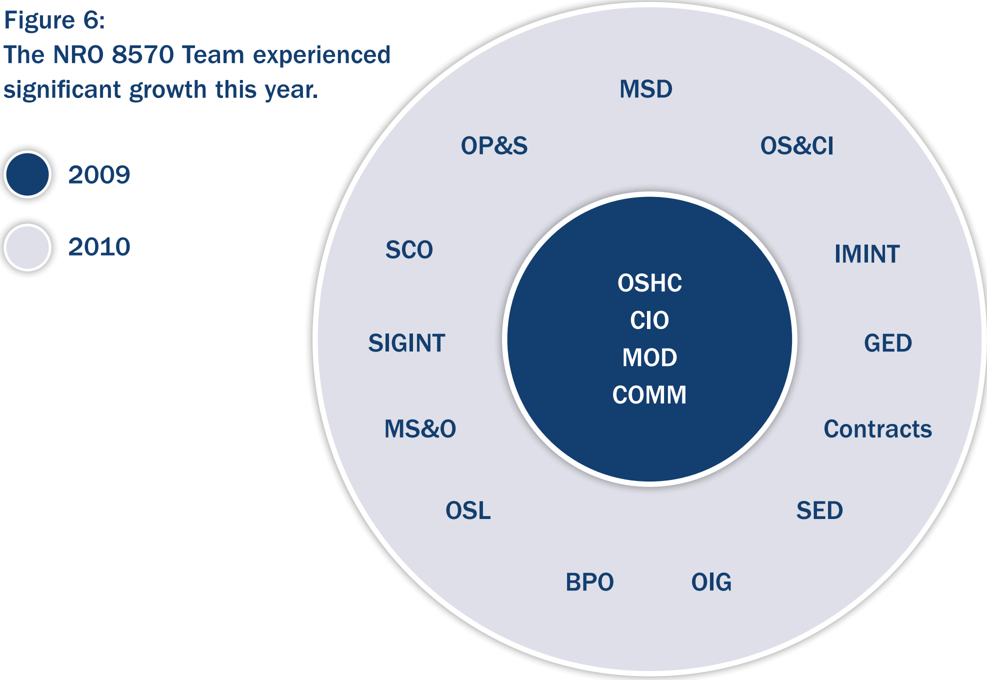
DoD 8570.01-M Information Assurance Workforce Improvement Program Compliance

The CIO submitted its first IA Workforce Improvement Program (IA WIP) Annual Report to the DoD CIO in January. This submission, summarizing calendar year 2009 data, represented a subset of the NRO IA workforce. During 2010, the NRO 8570 Team, comprised of representatives from all NRO Ds and Os, conducted an enterprise-wide IA assessment to identify all remaining IA positions and determine NRO's level of compliance with the full Directive. The IA workforce count increased from 471 in 2009 to 1334 in 2010. The NRO 8570 Team doubled its membership to 49 representatives from the Ds and Os during 2010.

This team will refine NRO IA Workforce assessments and explore best value training options to improve our overall 8570.01M compliance levels. In addition, the 8570 Team will continue to collaborate with the National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), Defense Intelligence Agency (DIA), Air Force, and Navy partners to identify best practices, coordinate training offerings, and address common DoD 8570.01M issues. Finally, the team is coordinating with OSHC to include DoD 8570.01M language in future position descriptions, and with the Office of Contracts to ensure DoD 8570.01M language is integrated into future requests for proposals.

2010 Major Accomplishments (continued)

**Figure 6:
The NRO 8570 Team experienced significant growth this year.**



Spectrum

On September 15, 2010, the Director of National Intelligence (DNI) designated the NRO as the Lead IC Element for coordinating spectrum activity in the IC. The DNI granted NRO this designation because of the highly-specialized spectrum expertise and years of experience that reside within the NRO CIO. With this new designation as the Lead IC Element, the NRO is responsible for chartering and chairing the Intelligence Community Spectrum Council (ICSC). The ICSC, comprised of representatives from each IC element, will monitor spectrum issues and make recommendations to the DNI for IC actions regarding potential reallocation of federal spectrum for commercial wireless use. In this new role, the NRO will bring the IC together to share processes, best practices, and information.

Within the NRO, the CIO hosted a Spectrum Requirements Conference (SRC) to discuss NRO project requirements and emerging technologies in conjunction with the increasing demand for access to the radio spectrum. Diligence is required in many areas in order for the CIO to provide information assurance for NRO communication links. In this forum, the SRC examines present and future communication technologies and other areas of National Security Space. This event is now in its third year, and has continued to have strong attendance and significant technical contributions. The next SRC will be held in June 2011.

Innovation

The CIO champions innovation through collaboration with internal and external organizations using forums, expos, technical exchange meetings, and pilots to broker agreements between organizations with like needs. In 2010, CIO piloted three new capabilities to enhance NRO IT innovation.

The CIO partnered with GED and Advanced Systems & Technology (AS&T) to pilot the Science & Technology Encyclopedia (SnTpedia) tool. Through SnTpedia, NRO explored a new way of discovering information on current and future research projects with the end goal of aggregating data for decision making and creating new linkages between projects. Implementation of SnTpedia will dramatically enhance NRO's ability to look into its science and technology

2010 Major Accomplishments (continued)

investments by exposing, discovering, and visualizing associated projects through wiki manipulation. The impact of this capability will be to allow disparate research and development projects to discover each other. Programs with like goals, objectives, and interests can enhance collaboration and reduce program overlaps.

The second pilot focuses on IA. Automated Vulnerability Assessment (AVA) provides the ability to automatically scan software executables to discover vulnerabilities. Implementation of AVA will change the way NRO certifies, accredits, and audits software through enhanced software assurance and portability used to support certification reciprocity and re-use. This capability will improve the NRO's ability to conduct software C&A, software portability and reciprocity, enterprise software re-use, and secure software quality assurance. CIO partnered with OS&CI, GED, SED, and COMM on this pilot.

The third pilot, Firefox® , is an open source modern browser that allows extensions and plug-ins to aid web developers in troubleshooting their software and provides a standards-based rendering of websites that is different from Microsoft® Internet Explorer® . Firefox® has been added to the NRO baseline. This allows NRO to take advantage of unique extensions and aids the transition of several systems that need access to a modern web browser. COMM, MS&O, and BPO played key roles in this effort.

CIO will continue its focus on innovation in 2011 as it pilots technologies in the areas of secure wireless, cloud computing, next generation desktop, 5-Eyes enterprise, and green IT.

Intelligence Community and Department of Defense Initiatives

Over the past year, CIO supported several IC- and DoD-wide initiatives to increase the efficiency and effectiveness of IT and promote information sharing.

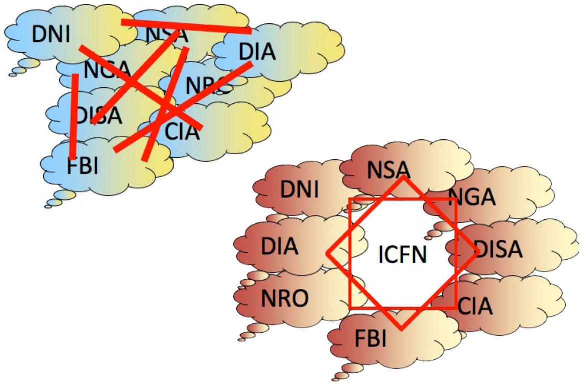
ODNI Business Transformation Office

The ODNI, Congress, and the IC formally established the Business Transformation Office (BTO) in October 2008 to leverage people, processes, and technology to transform the IC into an integrated and streamlined Intelligence Enterprise. Throughout 2010, the NRO CIO worked closely with BPO, MS&O, and the Acquisition Center of Excellence to provide support to a number of BTO initiatives. The CIO, by providing subject matter experts (SMEs), resources, and guidance, contributed to the development of an IC Business Enterprise Architecture (BEA) 2.0 that establishes the blueprint for the overall transformation effort. The BTO organized BEA Day to allow members of the community to preview the architecture and familiarize themselves with it prior to formal release. In addition to supporting BEA Day activities, the NRO CIO coordinated feedback on the BEA on behalf of the NRO. The BTO delivered the IC BEA to OMB and Congress in September 2010.

Intelligence Community Federated Network

The IC Network Integration Steering Group (NISG) established the IC Federated Network (ICFN) project to create an enduring architecture and methodology to interconnect IC elements more economically, robustly, and securely at the Top Secret/ Sensitive Compartmented Information (TS/SCI) level. ICFN aims to use existing network infrastructure to create peering points for IC elements to use for inter- and intra-agency connectivity to the SCI fabric. The project has many aspects that alone would result in enhancements for the IC:

Figure 7:
ICFN will advance interagency information sharing and collaboration.



2010 Major Accomplishments (continued)

- Inter-Network Operations Center Coordination and Collaboration;
- Implementing an Internet Protocol and Name registry;
- Developing network peering and implementation standards for interconnecting IC elements; and
- Implementing an IC-Wide Bandwidth and Capacity Management process.

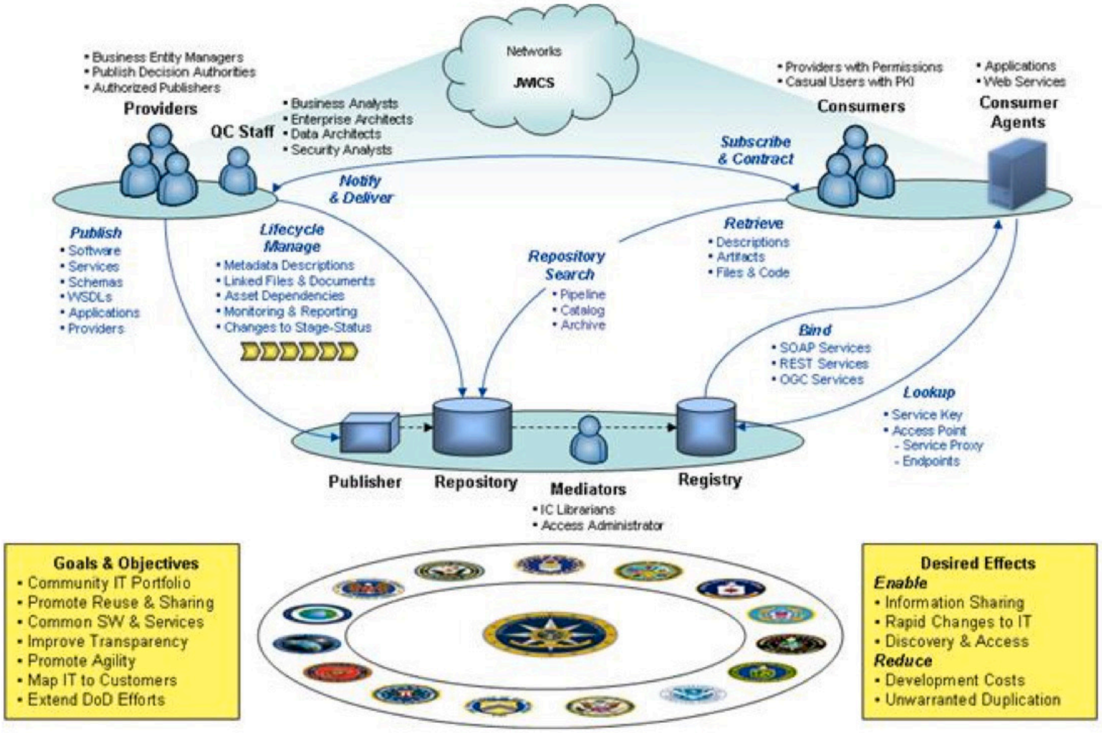
These combined achievements will create a sustainable network capable of providing TS/SCI access to IC elements independent of location, service provider, or parent agency.

The NRO is the designated lead agency for this project and the CIO has activated a Project Management Office, initiated contract actions to acquire staff support, and developed several significant programmatic documents for start-up of this project. This multi-year project includes direct support from DoD, NSA, NGA, Central Intelligence Agency (CIA), Department of State, Federal Bureau of Investigation, DIA, Department of the Treasury, Department of Homeland Security, and other IC elements, making it a true Community effort to bring the DNI's 2015 Vision of network integration to fruition. When complete, ICFN will enhance the ability of the entire IC to identify, share, and consume vital information across agency borders and in a timely manner.

IC Enterprise Registry and Repository

The CIO continued to champion NRO as a service provider for critical IC Core Services. The CIO, in a sponsorship role, supported GED as it developed, deployed, and operated the IC's Enterprise Registry and Repository (ER2). The IC CIO directed the NRO to serve as the Designated IC Element to stand up ER2 using funding from the ODNI. ER2 provides

Figure 8:
IC ER2 Operational Overview



2010 Major Accomplishments (continued)

developers and service providers a capability to share and reuse software and services. Sharing IT results in a reduction in custom development costs and the elimination of unwarranted duplication. The solution provides the same look and feel as the DoD DISA registry. This IC enterprise capability is delivered via the Joint Worldwide Intelligence Communications System.

The technical solution is designed and built to be extensible to support additional capabilities for community service reuse and information sharing requirements. New capabilities being added to ER2 include IC standards, service profiles, widgets, and content collections.

The ER2 system went live in May to a small set of early adopters from across the IC so they could begin loading a variety of community software and services into ER2, as well as test the features and components of the system. In September ER2 expanded to the full IC.

Intelligence Community IT Standards and Profiles

The IC Enterprise Standards Committee (ESC), with strong NRO CIO support, adapted DoD processes to create a baseline of standards and associated information to facilitate information-sharing capabilities for the IC, its partners, and its customers. The ESC released three updates of the IC Enterprise Standards Baseline in 2010: IC Standards Registry (ICSR) 10-1.0, 10-2.0 and 10-3.0. Three additional updates are planned for 2011.

With DNI and IC partners, NRO CIO led or significantly influenced the development of:

1) Intelligence Community Standard (ICS) 500-20 IC Enterprise Standards Governance, ICS 500-21 Tagging of Intelligence and Intelligence-Related Information, and ICS 500-27 Audit;
2) Processes for how ICSR and DoD IT Standards Registry (DISR) jointly catalog standards while respectively exposing and protecting classified content; and
3) IC Enterprise Standards Governance Terminology and Acronyms with References document.

The IC Standards Collaboration Forum, initially founded by NRO, NGA, and NSA to address areas of common interest related to standards and standardization activities and to leverage common solutions, has engaged the DIA, providing an opportunity to address standards-related issues affecting the four partners.

Joint Architecture Reference Model 2.0

The NRO CIO led a team from NRO, NSA, CIA, DNI, and DoD to update three components of the Joint Architecture Reference Model (JARM) — the Enterprise Competency Model, Enterprise Services List, and Technical Services Taxonomy. In addition, the team developed a training package and an Excel-based mapping aid for program management and investment personnel within the IC elements. The Joint Architecture Working Group (JAWG) approved this 2.0 version of the JARM in August.

Aligning IT investments with the JARM (a required part of IC Exhibit 300 submissions) allows the NRO to identify the technical and enterprise services that an investment will deliver, rely upon, and/or consume, along with the enterprise competencies required by the investment. By October, CIO trained the program managers of the NRO Exhibit 300 projects, resulting in a 100 percent success rate for mapping FY 2012 Exhibit 300 submissions to the JARM. NRO anticipates that aligning investments to the JARM will be required for IT Exhibit 53s in FY 2013.

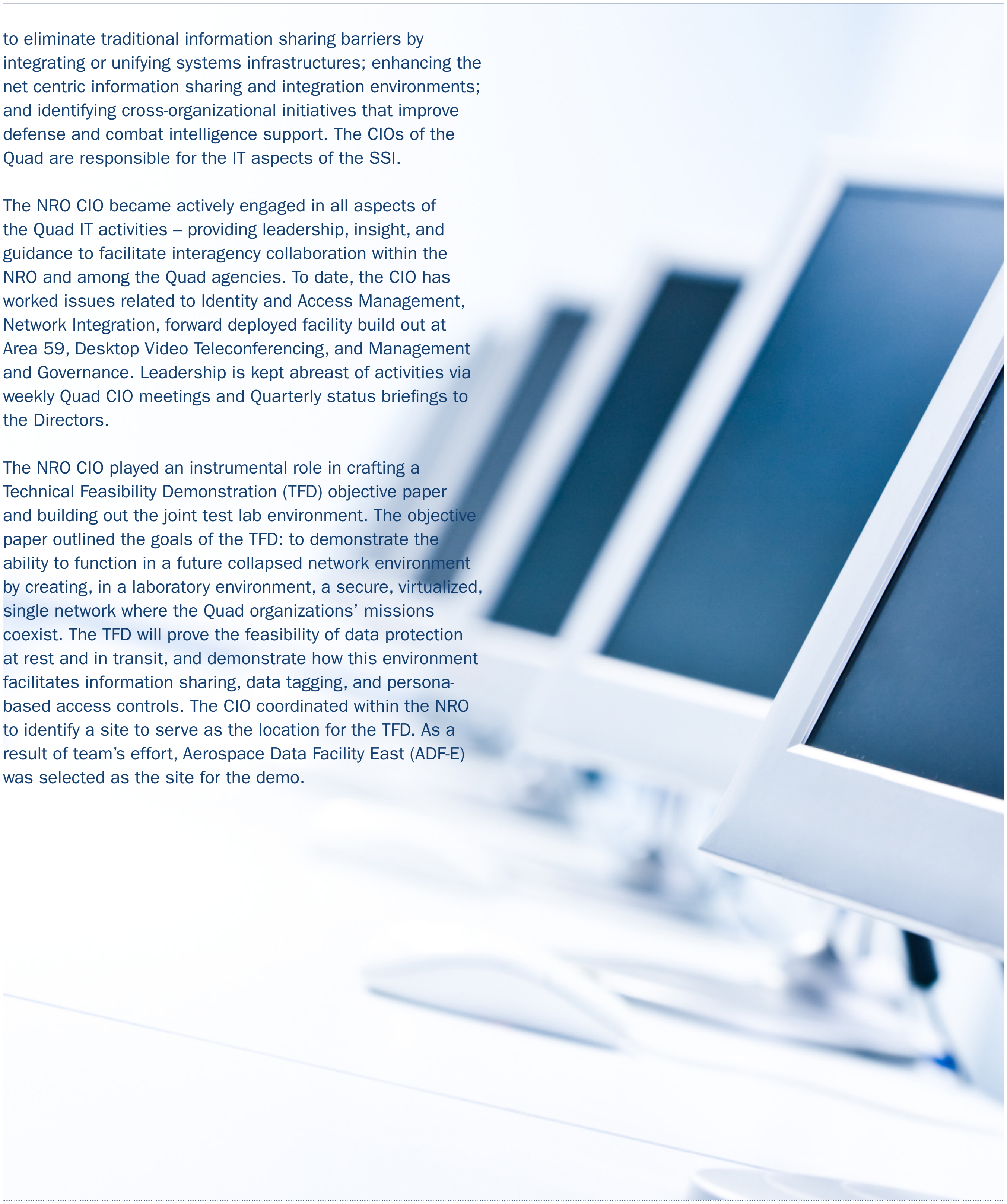
Shriever Wargame 2010

The CIO represented the NRO at the Schriever Wargame 2010, the sixth in a series of war games sponsored by Air Force Space Command. The wargame examined policy, strategy, Concepts of Operations, and architectural implications of threats to space (and, effective with this game, the cyber environment). Over 500 participants played the game. Participation by IC representatives was the most substantial to date. The MOD, GED, and OS&CI provided experts that aided a comprehensive cyber staff to represent the NRO. Because of the unique perspective of the IC representatives, the observations and insights brought to the game proved substantial and extremely helpful. The outcomes of the wargame provided new insight into NRO's role and support to both space and cyber operations. The NRO will use these outcomes to validate future architecture designs and strategies for space acquisition.

Quad

The "Quad" is a four organization collaborative partnership between the Directors of NRO, NSA, NGA, and DIA. It was codified in a 9 November 2009 Statement of Strategic Intent (SSI) Memorandum of Understanding, signed by the four Directors. The SSI aims

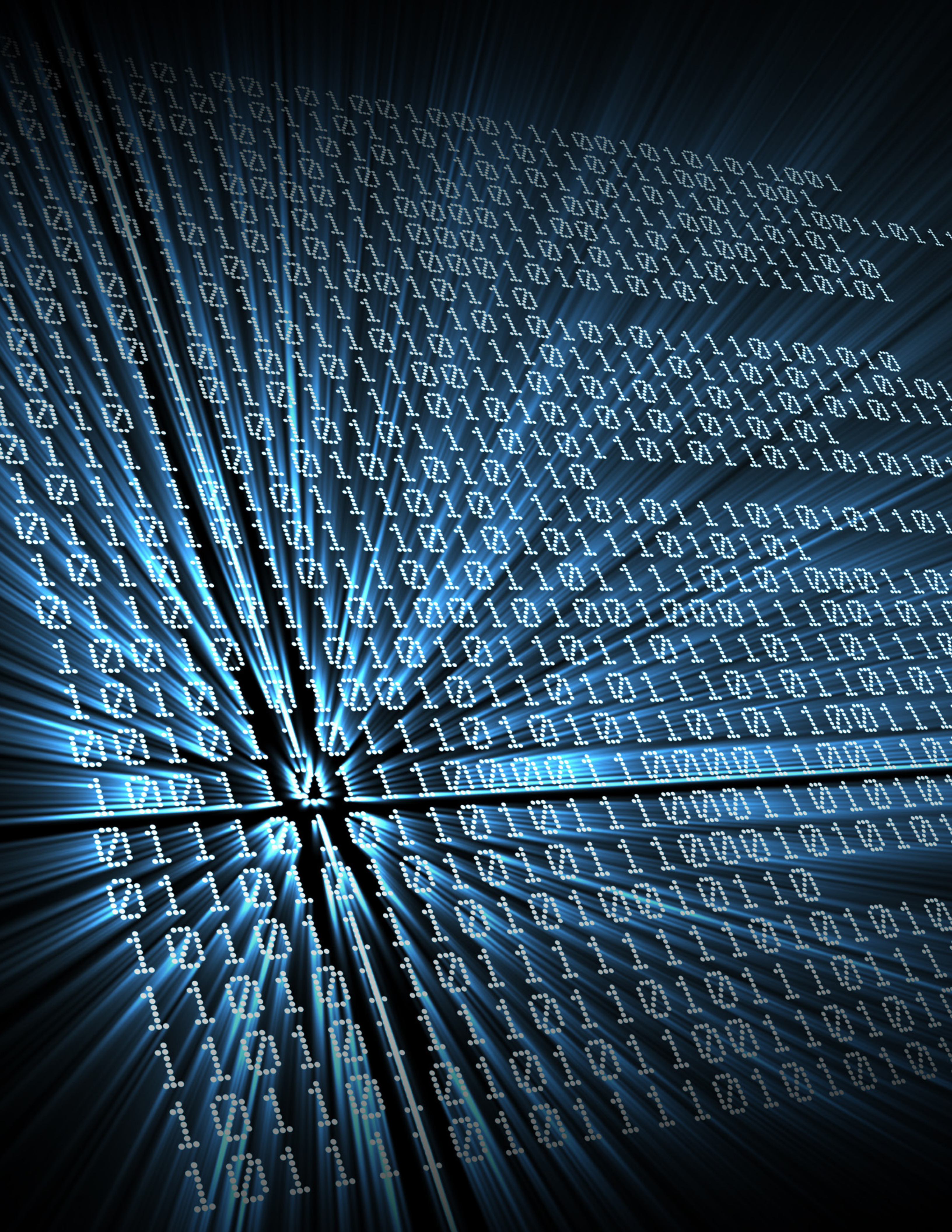
2010 Major Accomplishments (continued)



to eliminate traditional information sharing barriers by integrating or unifying systems infrastructures; enhancing the net centric information sharing and integration environments; and identifying cross-organizational initiatives that improve defense and combat intelligence support. The CIOs of the Quad are responsible for the IT aspects of the SSI.

The NRO CIO became actively engaged in all aspects of the Quad IT activities – providing leadership, insight, and guidance to facilitate interagency collaboration within the NRO and among the Quad agencies. To date, the CIO has worked issues related to Identity and Access Management, Network Integration, forward deployed facility build out at Area 59, Desktop Video Teleconferencing, and Management and Governance. Leadership is kept abreast of activities via weekly Quad CIO meetings and Quarterly status briefings to the Directors.

The NRO CIO played an instrumental role in crafting a Technical Feasibility Demonstration (TFD) objective paper and building out the joint test lab environment. The objective paper outlined the goals of the TFD: to demonstrate the ability to function in a future collapsed network environment by creating, in a laboratory environment, a secure, virtualized, single network where the Quad organizations' missions coexist. The TFD will prove the feasibility of data protection at rest and in transit, and demonstrate how this environment facilitates information sharing, data tagging, and persona-based access controls. The CIO coordinated within the NRO to identify a site to serve as the location for the TFD. As a result of team's effort, Aerospace Data Facility East (ADF-E) was selected as the site for the demo.



Looking Ahead

The Chief Information Office is proud of its 2010 accomplishments. The office's achievements within the CIO, NRO, and IC have moved NRO closer to achieving its goal of increasing IT value to the NRO mission. Looking ahead to 2011, NRO still faces many IT challenges that require focused attention, creative solutions, and collaborative efforts to solve. Four major drivers highlight the need for optimizing IT in the NRO:

1. The increased focus by the Director of National Intelligence and the Secretary of Defense on driving IT efficiencies within their organizations;
2. The commitment to dramatically improve integration as outlined in the Quad Statement of Strategic Intent;
3. The game-changing mission advantages IT offers; and
4. The increased need for better cyber defense of our IT systems.

With these drivers in mind, the NRO CIO completed an off-site in late 2010 to set clear priorities for 2011. The priorities are shown below:

Optimizing IT in the NRO will be a difficult task but it is necessary to take steps toward improving our IT performance and gaining full, tangible value from our IT by managing it better. The CIO plans to engage all Directorates and Offices in order to bring forward an overarching strategy for optimizing IT for the NRO Enterprise in 2011 and beyond.

NRO CIO 2011 Priorities	
Optimize NRO IT Workforce	Standardize NRO IT Project Management Lifecycle
Mature NRO IT Governance	Drive IT Efficiencies
Implement NRO IT Architecture	Create IT Requirements Management Process
Deepen IC and DoD Partnerships	Define CWAN Way Forward
Improve Information Assurance	Champion IT Services Catalog
Develop Technology Roadmaps	

Acronyms

ACIO	Associate Chief Information Officer
ADF-E	Aerospace Data Facility - East
AS&T	Advanced Systems and Technology
ATO	Approval to Operate
AVA	Automated Vulnerability Assessment
BEA	Business Enterprise Architecture
BPO	Business Plans and Operations
BTO	Business Transformation Office
C&A	Certification and Accreditation
CBPI	Corporate Business Process Instruction
CCRI	Command Cyber Readiness Inspection
CDS	Cross Domain Solutions
CDSO	Cross Domain Support Office
CIA	Central Intelligence Agency
CIO	Chief Information Office
CNSSI	Committee on National Security Systems Instruction
COMM	Communications Systems Directorate
D and O	Directorate and Office
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DNRO	Director, National Reconnaissance Office
DoD	Department of Defense
EIAP	Enterprise Information Assurance Program
ER2	Enterprise Registry and Repository
ESC	Enterprise Standards Committee
EVAR	Enterprise Vulnerability Assessment and Remediation
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GED	Ground Enterprise Directorate
IA	Information Assurance
IA WIP	Information Assurance Workforce Improvement Program
IASD	Information Assurance Standards Document
IC	Intelligence Community
ICD	Intelligence Community Directive

ICFN	Intelligence Community Federated Network
ICS	Intelligence Community Standard
ICSC	Intelligence Community Spectrum Council
ICSR	Intelligence Community Standards Registry
IG	Inspector General
IM	Information Management
IPA	Independent Program Assessment
IT	Information Technology
ITEC	Information Technology Executive Committee
IT-IA-IM	Information Technology-Information Assurance-Information Management
ITA	Information Technology Architecture Description
ITS	Information Technology Strategy
ITTG	Information Technology Transition Guidance
ITTP	Information Technology Transition Plan
JARM	Joint Architecture Reference Model
JAWG	Joint Architecture Working Group
MOD	Mission Operations Directorate
MSA	Major Systems Acquisition
MSD	Mission Support Directorate
MS&O	Management Services and Operations Directorate
NGA	National Geospatial-Intelligence Agency
NGE	NRO Ground Enterprise
NIPRNet	Non-classified Internet Protocol Routing Network
NISG	Network Integration Steering Group
NMIS	NRO Information Management System
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS&CI	Office of Security and Counterintelligence
OSHC	Office of Strategic Human Capital
PED	Portable Electronic Device
PKI	Public Key Infrastructure
PwC	PricewaterhouseCoopers

Acronyms

SED	Systems Engineering Directorate
SIPRNet	Secret Internet Protocol Routing Network
SME	Subject Matter Expert
SnTpedia	Science and Technology Encyclopedia
SRC	Spectrum Requirements Conference
SSI	Statement of Strategic Intent
TFD	Technical Feasibility Demonstration
TS/SCI	Top Secret/Sensitive Compartmented Information
VAR	Vulnerability Assessment and Remediation
VMWG	Vulnerability Management Working Group

NATIONAL RECONNAISSANCE OFFICE
CIO
CHIEF INFORMATION OFFICER

NRO CIO on NMIS: http://ocio
NRO CIO on Intelink: https://www.nro.ic.gov/ocio