U.S. Government Continuity of Operations Planning (COOP):

Legislative Overview and Selected Federal Case Studies

A White Paper Prepared for Symantec Corporation

April 17, 2006

FedSources
A WASHINGTON MANAGEMENT GROUP COMPANY

Table of Contents

Introduction

The US federal government, in addition to being the largest consumer of information technology in the world (with a FY07 IT budget exceeding $63.8 billion), is the single largest holder of the nation's most sensitive medical, financial, and law enforcement-related data. Beyond structural damage and loss of life, the amount of chaos that could be inflicted upon the US economy – and by extension world economy – by a destructive device in or around any one of several key federal agencies' IT centers is nearly impossible to predict.

The purpose of this white paper is to provide COOP professionals with an understanding of the current legislative and policy environment surrounding COOP, as well as recommendations for optimizing the effectiveness of an agency's COOP plan within this environment (Part 1). Additionally, this paper will highlight several significant case studies illustrating ways in which COOP is being implemented today by key federal agencies who are leading by example (Part 2).

The volume of sensitive data being processed by the federal government continues to increase at a rapid pace. To cite just a few examples, the Social Security Administration currently tracks payroll contributions from more than 158 million working Americans and processes monthly benefit checks for over 48 million recipients.[1] Additionally, today more than half of all Americans file their taxes electronically with the IRS, which processes a total of nearly 227 million income tax returns annually.[2] Finally, Medicare and Medicaid currently insure more than 25% of the country's population, with Medicare alone processing more than one billion claims per year.[3] The loss of the data from one of these or many other key federal agencies would be nothing short of catastrophic, costing several billions of dollars and affecting the lives of hundreds of millions of citizens.

From just these examples above, it can be clearly seen that merely protecting federal data centers from harm is not enough. As this white paper will illustrate, because the risk associated with widespread data loss at government agencies is so high, federal CIOs and recovery experts are being called upon to assume a leadership role in ensuring that key data stores will not be lost, even in the event of a severe and prolonged disruption. To this end, the individual agencies have developed risk mitigation plans against information loss (*e.g.,* establishing archiving and recovery procedures, redundant storage systems, parallel communication links, *etc*.), known collectively as "Continuity of Operations" (COOP) planning.

[1] http://www.ssa.gov/barnhart.htm
[2] http://www.irs.gov/newsroom/article/0,,id=150358,00.html, http://www.taxpolicycenter.org/TaxFacts/TFDB/TFTemplate.cfm?Docid=18
[3] http://www.hhs.gov/about/whatwedo.html

Executive Summary

Part 1: Legislative Overview

- In recent decades, the federal government has worked to update and streamline the guidance it provides to agency IT managers for ensuring the efficient management of IT resources, including Disaster Recovery and Continuity Planning. Of ten primary COOP directives issued since 1996, the key directives that govern COOP planning today have all been written or revised since September 11th, 2001.

- Federal Preparedness Circular (FPC) 65 remains the central policy document for current COOP planning.[4] This circular, originally issued in 1999 and updated in 2004, outlines the specific requirements for each agency's COOP plans and assigns the Federal Emergency Management Agency (FEMA) as the government's lead department for COOP coordination.

- In addition to FPC 65, two recent DHS-issued reports – the *Homeland Security National Response Plan* (NRP) and the *National Infrastructure Protection Plan* (NIPP) – provide greater detail for agencies on the roles that each organization plays in the national federal infrastructure protection and disaster response plan.[5] These documents identify DHS's Information Analysis and Infrastructure Protection Directorate (IAIP) as the lead organization in charge of COOP planning coordination for telecommunications and IT infrastructure.

- Recently-introduced documents, such as DHS's *Intelligence Enterprise Strategic Plan*, indicate the ways in which DHS is expanding its COOP leadership role beyond the traditional civilian agencies and into the intelligence community (e.g., CIA, NSA).

- Based upon an analysis of the current COOP policy environment and trends, FedSources offers the following key recommendations for federal COOP professionals (see *Recommendations* section for additional details):

  1. *COOP professionals should ensure that they are taking steps to create comprehensive (and continually-updated) continuity plans that are in accordance with FPC 65 and other DHS-issued guidelines.*
  2. *Once a disaster recovery prioritization assessment is completed, agency COOP professionals should architect, implement, and test an IT continuity plan in partnership with an experienced IT integrator with tested COOP solutions.*
  3. *COOP professionals should address issues of security and availability concurrently.*
  4. *COOP professionals should anticipate the need to provide telecommuting and secure remote access services as an increasingly central component of an agency's continuity and recovery plan.*
  5. *Looking forward, COOP professionals should incorporate the lessons of FISMA and prepare for increased standardization, documentation, and evaluation.*

[4] FPC 65: http://www.fema.gov/onsc/docs/fpc_65.pdf
[5] NRP: http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf; NIPP: http://www.ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf

Part 2: Selected Federal Case Studies

The following federal agency COOP case studies were selected for this white paper on the basis of the size of these agencies' IT budgets, as well as the mission-criticality of their infrastructures. In addition, these three organizations are examples of agencies that are helping the Administration to achieve success in some of its key mission areas, including: Homeland Security, Space Exploration, and Budget Management.[6]

To illustrate how these missions are being supported today by their lead agencies in the areas of continuity planning and disaster recovery, the federal agencies highlighted in this white paper include: the Department of Homeland Security (DHS), the National Aeronautic and Space Administration (NASA), and the Internal Revenue Service (IRS).

A summary of the key conclusions from these three case studies appears below.

- DHS has taken on a significant COOP challenge, because in part, each of its original 22 component agencies have highly diverse IT continuity and disaster recovery requirements. Recent Congressional legislation is pushing DHS to modernize its COOP planning and execution agency-wide, while departments such as the Coast Guard (USCG), the Bureau of Customs and Border Protection (CBP), and the Federal Emergency Management Agency (FEMA) have all taken steps to implement a localized COOP plan in coordination with consultants and IT providers. While these COOP efforts have been successful, government auditors have recently indicated areas to DHS where greater attention is needed.

- NASA views its COOP objectives from the perspective of the manned and unmanned missions being coordinated by its various space flight centers and other major facilities nationwide. As a result, each NASA installation has been given the contracting authority to procure the COOP facilities, equipment, and services is requires to keep constantly available the extremely high-resolution images, complex data models, and other sensitive electronic assets NASA facilities require to make its missions a success.

- IRS has seen its COOP planning and infrastructure evolve significantly since September 11, 2001, partly in response to studies which have measured the effects of disruptions to IRS's electronic tax return processing systems in the tens of millions of dollars per week. Over the past five years, the Treasury sub-agency has created an integrated Mission Assurance team responsible for IT security, physical security, and business continuity across the IRS's more than 700 field offices. The IRS tests its COOP system periodically, and uses outside research firms such as MITRE Corporation to conduct detailed COOP system assessments and recommend updates in accordance with FEMA policy.

[6] http://www.whitehouse.gov/infocus/

Part 1: Legislative Overview

Background

While federal government programs for the archiving and recovery of its data resources began with the installation of the first mainframes several decades ago, modern COOP policy only became the subject of Executive Branch-level orders beginning in the late 1980s. Throughout the 1990s, as disaster recovery and business continuity services began to gain popularity in the private sector, the government began to more formally codify responsibilities among the federal agencies for the management of critical IT resources, including the development of plans to ensure system availability following service interruptions (*e.g.,* natural disasters, power outages, fires, or floods).

With the establishment of the Department of Homeland Security (DHS) in 2002, the administration had a lead cabinet-level agency (and within it the Federal Emergency Management Agency, or FEMA) to direct federal COOP planning and execution to both prepare for and respond to natural and man-made disruptions. At that time, DHS was chartered not only with overseeing government agencies' continuity plans but also coordinating best practices with IT security and recovery experts from the private sector.

The legislative branch has been increasing its oversight of federal agencies' COOP progress in recent years. In April 2005, the House Government Reform Committee, Chaired by Congressman Tom Davis (R-VA), held a hearing to review the federal government's IT disaster recovery plans entitled, *Who's Watching the COOP? A Re-Examination of Federal Agencies' Continuity of Operations Plans.* During an April 2004 hearing, the Government Reform Committee had found "significant inadequacies" in the federal COOP process and Chairman Davis raised concerns that the federal government may not be able to remain fully functional in the event of a severe natural disaster, terrorist attack or other emergency.

The Government Reform Committee hearing also revealed that while many agencies had some form of a COOP plan in place, only a small percentage of agencies were implementing the newest COOP planning recommendations, including following the guidance from the Office of Personnel Management (OPM) to implement a telecommuting plan that would allow employees to securely access IT resources from home or other remote locations in the event of an emergency. A GAO report cited in the hearing revealed that fewer than 12% of federal employees could work remotely for any extended period during an emergency if required to do so today – a number which Congress feels should be doubled.[7]

[7] *Continuity of Operations: Agency Plans Have Improved, but Better Oversight Could Assist Agencies in Preparing for Emergencies* (GAO 05-577) April 2005.

The COOP Policy Landscape Today

The table below outlines the key documents that comprise the current federal COOP policy environment (see Table 1).

Table 1: Timeline of Key Federal COOP Directives and Plans

#	Title	Date
1	*National Infrastructure Protection Plan (NIPP)* (Draft v2.0)	Released for Comment: Jan. 2006
2	*DHS Intelligence Enterprise Strategic Plan*	Issued: Jan. 2006
3	*Department of Homeland Security National Response Plan (NRP)*	Issued: Dec. 2004
4	Federal Preparedness Circular 65: *Federal Executive Branch Continuity of Operations*	Updated: Jul. 2004 (Original: Jul. 1999)
5	Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*	Dec. 2003
6	*The National Strategy to Secure Cyberspace*	Feb. 2003
7	Homeland Security Presidential Directive 5: *Management of Domestic Incidents*	Feb. 2003
8	Presidential Decision Directive 67: *Enduring Constitutional Government and Continuity of Government Operations*	Oct. 1998
9	Presidential Decision Directive 63: *Critical Infrastructure Protection*	May 1998
10	OMB Circular A-130: *Management of Federal Information Resources*	Feb. 1996

Note: For additional status information and a more detailed summary of each of the policy documents listed in Table 1 above, please see *Appendix A*.

While several types of COOP-related documents have been issued since the early 1990s, all federal directives and orders related to infrastructure protection and COOP have had at their core, one or more of the following five key objectives:

1. Raise the awareness of the need for effective COOP planning among agency CIOs and CTOs
2. Establish a common COOP vocabulary across all agencies
3. Establish a lead coordinating agency (now FEMA) and outline roles and responsibilities for all those involved in the COOP effort government-wide
4. Encourage each agency's IT department to identify its most crucial assets
5. Encourage each agency to document ways in which these assets will be protected from loss and normal operations will continue in the wake of a disruptive incident

A brief overview of two of the most significant areas within the COOP policy environment follows below.

Federal Preparedness Circular 65

- Of the nine key COOP documents outlined in Table 1 above, the central directive driving COOP planning at the agency level today is Federal Preparedness Circular 65: *Federal Executive Branch Continuity of Operations* (FPC 65). Originally issued in July 1999, FPC 65 was updated in July 2004 to reflect post-9/11 COOP strategies, technologies, and governmental structures.

- All valid agency COOP plans today must be FPC 65 compliant, and among other requirements must include detailed procedures in each of the following areas:

- Plans and Procedures
- Identification of Essential Elements
- Delegations of Authority
- Orders of Succession
- Alternate Facilities
- Interoperable Communications
- Vital Records and Databases
- Tests, Training, and Exercises

- The updated 2004 version of FPC 65 also includes among its new sections a *Reconstitution Annex* with directions to agency CIOs to detail plans for returning employees and other IT resources to original facilities and operational status after a disruptive event has passed.

The Presidential Directives and Resulting Reports

Beyond FPC 65, over the past several years a number of other post-9/11 White House directives, known as *Homeland Security Presidential Directives* (HSPDs), have preceded the publishing of two reports that outline national COOP plans for agency-level CIOs and CTOs in greater detail.

- First, HSPD 5 *(Management of Domestic Incidents)* called for the creation of the *Department of Homeland Security National Response Plan* (NRP), issued in December 2004.
  - The NRP divides the total US economy into various sectors and places DHS's Information Analysis and Infrastructure Protection Directorate (IAIP) as the department in charge of coordinating COOP planning for the government's telecommunications and IT infrastructure.
  - Under the plan, agencies are asked to participate in the government-wide effort by appointing COOP coordinators to the Interagency Incident Management Group (IIMG), a headquarters-level group which convenes when the President directs DHS to assume incident management responsibility. Agency heads are also asked to make COOP staff available as required during an emergency to the Homeland Security Operations Center (HSOC).

- Additionally, HSPD 7 *(Critical Infrastructure Identification, Prioritization, and Protection)* called on DHS to create the *National Infrastructure Protection Plan (NIPP)* (draft released for comment November 2005.)
  - The NIPP was created as a comprehensive document to describe each agency's role in protecting the Critical Infrastructure/Key Resources (CI/KR) of the US. Like the NRP, it specifies DHS (and its Cyber and Telecommunications Security group) as the coordinator for IT and telecommunications security.
  - Under the NIPP, agencies are requested to nominate COOP experts as Homeland Security Advisors (HSAs) to assist DHS in developing and coordinating government-wide COOP plans. The HSA System is designed to provide a bridge between the "steady state" operations within the NIPP framework and the emergency incident management activities as described under the NRP (see above).

- Finally, the *National Strategy to Secure Cyberspace* (NSSC) (issued February 14, 2003), written for both a public and private sector audience, is not a policy document but instead offers recommendations to industry, higher education, and individual users of technology for securing their own IT systems. The NSSC also called for the creation of a National Cyberspace Security Response System (NCSRS), a partnership program between government and industry, coordinated by DHS, for managing incidents of national significance. In 2004, the NCSRS became chartered with providing subject-matter expertise on cyber threats to the IIMG (see above).

Recommendations

Within the framework of the COOP policy environment summarized above, FedSources offers the following recommendations for federal COOP professionals:

1. COOP professionals should ensure that they are taking steps to create comprehensive (and continually-updated) continuity plans that are in accordance with FPC 65 and other DHS-issued guidelines.

   Before finalizing a COOP plan, agency CIOs should familiarize themselves with both the most current continuity and recovery-specific best practices at an IT infrastructure level, in addition to the latest FEMA guidelines at the policy level. To help agency COOP coordinators create recovery plans that are both effective and compliant, FEMA provides a COOP self-assessment tool at:

   - http://www.fema.gov/government/coop/coopassessment3.shtm

   FEMA also provides a COOP planning template tool at:

   - http://www.fema.gov/doc/government/coop/coop_plan_blank_template.doc

2. Once a disaster recovery prioritization assessment is completed, agency COOP professionals should architect, implement, and test an IT continuity plan in partnership with an experienced IT integrator with tested COOP solutions.

   In response to urgings from Congress and FEMA, several federal agencies have moved their COOP design and implementation plans forward in recent months by seeking help from private sector experts. The table below lists key examples of COOP-related projects for which agency CIOs have recently issued early stage Request for Information (RFI) and Request for Proposal (RFP) announcements (see Table 2).

Table 2: Federal Agency COOP Solicitation Announcements, Sept. 2005 - Jan. 2006

Agency	COOP Project Title	Date Issued
Veterans Affairs	Support of R&D Computer Center Database	Jan. 26, 2006
Army – Defense Contracting Command	DCC-W Continuity of Operations Plans (COOP)	Nov. 10, 2005
Transportation	Disaster Recovery/Continuity of Operations	Nov. 1, 2005
Veterans Affairs	Drop Ship/Automation Center Disaster Recovery	Sept. 15, 2005

Source: FedSources Federal Opportunities Database, March 2006

3. COOP professionals should address issues of security and availability concurrently.

   During continuity and recovery planning, an agency's Chief Information Security Officer (CISO) and staff should be involved from the very beginning stages. This is because government information that is available but not secure in the wake of a disruption will be viewed at the minimum as untrustworthy and possibly in criminal violation of federal data privacy laws and associated compliance mandates. For example, the Department of Health and Human Services (HHS) is bound by Health Insurance Portability and Accountability Act (HIPAA) privacy requirements at all times, and the classified intelligence agencies also have strict requirements for data security. Additionally, data that is highly trusted, yet unavailable following a disruption is also useless. For these reasons, COOP professionals, in coordination with the CISO, should ensure that the IT providers selected for continuity projects are skilled in security technologies such as public key infrastructure (PKI), encryption, and authentication solutions. By considering security and availability in tandem, agencies will help maximize the overall integrity of their data.

4. COOP professionals should anticipate the need to provide telecommuting and secure remote access services as an increasingly central component of an agency's continuity and recovery plan.

   The April 2005 House Government Reform hearing on federal COOP preparedness revealed that moving forward, agencies will be required to demonstrate means by which federal employees will be able to work remotely for 30 days or more in the event of a physical disruption (*i.e.,* telecommuting). The Office of Personnel Management (OPM) recently reported that while the number of federal employees who worked remotely increased 37 percent from 2003 to 2004, 12 agencies still did not have a telecommuting policy in place at the beginning of 2005.[8] Most recently, existing telecommuting plans in the state of Louisiana have been shown to be inadequate in the wake of Hurricane Katrina, as the state's plans had been designed for minimal disruptions (if any) to physical infrastructure at the headquarters location.[9] Remote access or telecommuting plans in the future will thus need to account for potential communication outages at or around a disaster site, as well as physical damage to central IT systems.

   Moving forward, as telecommuting becomes a required component of an agency's COOP plan, agency COOP coordinators will need to demonstrate that access to key federal IT resources can be accomplished not only remotely but also highly securely – just as in the core IT system (see recommendation above). Thus, an agency's COOP IT provider should have expertise in not only premises-based security technologies, but virtual private network (VPN), Secure Sockets Layer (SSL) encryption, and other secure remote access technologies as well.

5. Looking forward, COOP professionals should incorporate the lessons of FISMA and prepare for increased standardization, documentation, and evaluation.

   While today the Federal Information Security Management Act (FISMA) program for federal cybersecurity preparedness has a more established evaluation system (with "A" through "F" grades issued annually in accordance with the agency's level of

[8] http://www.telecommuting.gov/documents/tw_rpt05/status-intro.asp

[9] http://www.govexec.com/story_page.cfm?articleid=32893&dcn=e_tcmg

compliance[10]), it can be anticipated that a similar system will emerge in the near future for the evaluation of an agency's COOP compliance, measured potentially against National Institute of Standards and Technology (NIST) and other FEMA-issued benchmarks. In preparation, agency COOP coordinators should ensure that continuity plans are well documented and ready for future GAO and congressional reviews.

Increased standardization of federal IT recovery plans has been foreshadowed by bills such as the *Continuity of Operations Demonstration Project Act* (HR 4797), currently under review by House Government Reform Committee, as a measure designed to test COOP plans on a government-wide basis, increase standardization, and promote best practices across agencies (see *Appendix A* for additional details on proposed COOP-related legislation).

[10] http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf

Part 2: Selected Federal Case Studies

Introduction

In January 2005, President Bush and his cabinet Secretaries outlined several high-profile mission areas for the President's second term. Three of these top administration programs and initiatives were the following:

- Homeland Security
- Space Exploration
- Budget Management[11]

As a result, to help achieve these and other key presidential priorities and objectives, there are few federal agencies with missions more critical than the Department of Homeland Security (DHS), the National Aeronautic and Space Administration (NASA), and the Treasury Department's Internal Revenue Service (IRS).

Within these key agencies, the CIO's top priorities include data security and availability, including continuity and disaster recovery planning. The proceeding chapter presents summary profiles of the COOP initiatives at these three mission-critical agencies, including some key challenges the agency is facing in response to today's new threat environment.

The agencies highlighted in the following case studies are serving as COOP role models for other agencies which are using the same FEMA guidelines to address their own specific availability and continuity needs. To help meet their COOP planning objectives, as well as those in other data integrity areas (*e.g.,* cyber-security), federal agencies will be looking more frequently to IT integrators (selected examples today include: SAIC, IBM and Booz Allen) as well as IT hardware and software partners with COOP expertise to help them ensure that their infrastructures are comprised of leading-edge products.

[11] http://www.whitehouse.gov/infocus/

Department of Homeland Security

FY06 Appropriated Budget: $31.9 billion	
IT Requested Budget, FY06: $3.64 billion	IT Requested Budget, FY07: $4.16 billion
Employees (US): 157,892	Employees (Total WW): 162,132
Chief Information Officer: Mr. Scott Charbo	

Introduction

Under the federal government reorganization that followed in the wake of the September 11th attacks, the Department of Homeland Security (DHS) became the lead federal agency for COOP planning. In March 2003, DHS assigned the responsibility of lead COOP agent to its emergency response sub-agency, the Federal Emergency Management Agency (FEMA). Under the current structure, DHS's FEMA is responsible for issuing COOP guidance and promoting understanding of and compliance with COOP requirements as detailed in Federal Preparedness Circular (FPC) 65 (see section above for details). FEMA's Office of National Security Coordination (ONSC) is DHS's implementing organization for its COOP lead agent responsibilities.[12]

However, in addition to coordinating the COOP planning for all federal agencies nationwide, DHS must also plan and implement disaster recovery and continuity planning for its own departments and directorates. To accomplish this objective, DHS's Chief Technology Officer, Lee Holcomb, former CIO of NASA, was brought into the organization with a deep institutional knowledge of federal COOP issues and solutions. In this mission, Mr. Holcomb works closely alongside DHS's CIO, Scott Charbo.

DHS's own COOP plan came into its most recent form through some assistance from Congressional statute. In October, 2005, Rep. Bennie Thompson of Mississippi introduced the Department of Homeland Security Reform Act of 2005 (HR 4009).[13] The Act proposed a top-level COOP strategy for DHS, which included a "telecommuting" (or telecommuting) solution, a policy which the US Office of Personnel Management (OPM) was charted with promoting among all federal agencies as a key COOP component. The Act proposes, within DHS's Office of Intelligence Analysis (OIA), an internal COOP plan with the following characteristics:

1. DHS's COOP plan will assure that the capability exists to continue uninterrupted intelligence analysis, collection, and related functions during a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies, that is maintained at a high level of readiness and is capable of implementation with and without warning.

2. DHS's COOP plan will include plans and procedures governing succession to office within the OIA, including:

[12] http://www.fema.gov/onsc/

[13] *Department of Homeland Security Reform Act of 2005* (HR 4009), October 6, 2005. Note: This legislation is still under review and on October 7, 2005 was referred to the House Committee on Transportation and Infrastructure's Subcommittee on Highways, Transit and Pipelines.

a. Emergency delegations of authority
b. The safekeeping of vital resources, facilities, and records
c. The improvisation or emergency acquisition of vital resources necessary for the performance of operations of DHS
d. The capability to relocate essential personnel and functions to and to sustain the performance of the operations of the Office at an alternate work site (*e.g.,* via telecommuting) until normal operations can be resumed[14]

Within this top-level COOP framework, DHS's many diverse sub-agencies have taken steps to address continuity and disaster recovery needs specific to their own individual structures, missions, and geographies. Three key examples of sub-agency COOP initiatives and challenges across the Department of Homeland Security are described below.

US Coast Guard (Number of employees: 7,198)

With its mission of projecting more than 95,000 miles of shoreline, the former military branch known as the US Coast Guard has very specific needs relating to COOP and IT continuity. To help it meet its objectives, USCG maintains two master communications centers, located in different parts of the US, which it uses for long-distance voice and data communications with vessels and public ships. In the event of an outage at one of these facilities, the USCG has backup facilities nearby that can assume continuity of operations.

In addition to the redundant sites and links mentioned above, the USCG also maintains three mobile Transportable Command Centers (TCCs), *i.e.,* trailers outfitted with radio and military satellite equipment and their own power generation. The equipment on these trailers, implementing technologies developed by the government at Sandia National Labs, employs a number of commercial satellite companies and also provides links to the USCG backbone network. After Hurricane Katrina, these TCCs were dispatched to the Gulf Coast to help with disaster relief. For more advanced COOP situations in the future, the USCG has also constructed a prototype scaled-down, suitcase-sized "kit" version of its TCC for handling phone and Internet access in the event of a disruption or emergency.[15]

Customs and Border Protection (Number of employees: 41,849)

In January 2002 (while still an agency of the Treasury Department), the US Customs Service – now DHS's Customs and Border Protection (CBP)) – solicited and awarded a contract for COOP services. While CBP did not release the names of the selected providers due to national security concerns, the terms of the solicitation stated that CBP was seeking a close-knit team of small businesses.[16] The contract, entitled *Disaster Recovery and Data Replication*, included the following specific COOP requirements:

1. Establishment of a Primary COOP facility, to be located between 20 miles and 350 miles from CBP's offices in Springfield, VA. The facility was to include computer-ready infrastructure (*i.e.,* raised floor, air conditioning, chilled water,

[14] Ibid.
[15] *Got COOP?*, Government Computer News, November 21, 2005, *http://www.gcn.com/24_33/tech-report/37569-1.html?topic=technology_products*
[16] FedSources Contracts Database, FSI #FSI0005611

power, automatic fire detection and suppression systems, and pre-positioned communications facilities).

2. Establishment of a Secondary COOP facility, to be located greater than 350 miles from Springfield, VA and not within the same city as the Primary facility.

3. Both the Primary and Secondary facilities were to provide the capability to replicate 21 terabytes of data stored on a Hitachi 7700E and 9960 Direct Access Storage Device (DASD). The timeline of recovery for the data was to be as close to the time of the disruption as possible and all data must be made available for use immediately and not more than 24 to 36 hours old.

This contract description above provides a useful illustration of the types of commercial equipment (*e.g.,* Hitachi storage DASDs) this group with DHS is using for its COOP facilities, and the size requirement of 21 terabytes of storage also indicate the scale of the recovery effort involved in an agency which has nearly 42,000 employees, yet only a small percentage based in the Washington DC metro area.

Federal Emergency Management Agency (Number of employees: 22,738)

Recently, one of FEMA's high-profile database systems came under scrutiny from the agency's Inspector General (IG) for its level of COOP preparedness. In the summer of 2005, Richard Skinner, DHS's Inspector General concluded that DHS's primary database for emergency preparedness and response lacked adequate COOP plans and protections for sensitive data. This system, known as the National Emergency Management Information System (NEMIS), tracks incident coordination efforts at FEMA's Emergency Preparedness and Response Directorate.

FEMA officials are currently using the database to manage disbursements to Katrina and other disaster victims as well as spending on recovery efforts at the federal and state levels. The Inspector General noted in his report that the directorate might not be able to recover the database after a disaster or major disruption and recommended that the DHS CIO's office create and implement annual contingency training and COOP testing programs. The NEMIS coordinators responded to the IG report, citing a lack of technical expertise and funding at the FEMA directorate.[17]

Conclusions

Like many other enterprise IT functions at the Department of Homeland Security, COOP planning and execution authority today still largely rests in the hands of the 22 component agencies that were integrated into DHS following the events of September 11th. The charter of providing continuous availability for such a heterogeneous and geographically diverse infrastructure has presented (and will continue to present) challenges to DHS, with groups like the Coast Guard (formerly a military branch) and the Customs and Border Protection sub-agency (to cite just two examples) having completely different COOP needs. As a result, DHS will continue to turn to outside homeland security IT experts and IT providers to ensure that any future disruptions caused by terrorist attacks meet with the most resilient federal IT infrastructure possible.

[17] *DHS Disaster Response Database Falls Short*, Federal Computer Week, November 14, 2005, http://www.fcw.com/article91405-11-14-05-Print

Recommendations

Based upon the findings in the case study above, FedSources offers the following recommendations for COOP professionals:

1. In an organization which is highly diverse (*i.e.,* with regards to mission, geography, and culture), it is important to make sure that each sub-unit's IT coordinator is using FEMA-authorized and standardized COOP templates and FPC 65-compliant policies. While templates can be adapted to meet a department's unique COOP needs (*e.g.,* US Coast Guard), agencies should not allow adaptation to evolve to a stage where IT managers are not leveraging best practices and even potentially risking non-compliance with FEMA and OPM policies.

2. Geographically dispersed organizations can benefit greatly from leading-edge remote monitoring tools that allow for 24-hour detection of potential disruptions, even before outages occur. DHS's National Emergency Management Information System (NEMIS) is one example of an agency system whose COOP preparedness status could be significantly enhanced with only a moderate increase in overall cost by employing remote management, backup, and archiving tools that could help monitor the NEMIS system automatically during and after business hours, ensuring the continuous availability of this critical data.

National Aeronautic and Space Administration

FY06 Appropriated Budget: $16.5 billion	
IT Requested Budget, FY06: $2.34 billion	IT Requested Budget, FY07: $2.23 billion
Employees (US): 18,771	Employees (Total WW): 18,786
Chief Information Officer: Ms. Patricia L. Dunnington	

Introduction

While the National Aeronautic and Space Administration (NASA) continues to expand the frontiers of both space and scientific understanding through its manned and unmanned missions, some recent tragedies have made NASA's need for data integrity, availability, and continuity more important than ever before. To this end, NASA's headquarters in Greenbelt, MD and its key installations nationwide have taken steps to help ensure that the space agency's critical data is secure and highly-available.

NASA's Office of Security Program and Protection (OSPP) is responsible for COOP planning and execution at the space agency. OSPP provides policy formulation, oversight, coordination, and management of following agency-wide programs, including two continuity-specific areas of responsibility (highlighted in the final two bullets below):

- Security
- Classified information management
- Unclassified information assurance
- COMSEC
- Counterintelligence (CI)/Counterterrorism (CT)
- Threat analysis
- Investigations (in conjunction with FBI)
- Homeland Security Research & Development liaison
- *Emergency Preparedness and Response*
- *Continuity of Operations (COOP)*[18]

Following the attacks of September 11th, former CIO Lee Holcomb was outspoken regarding the need for federal architectures to emphasize the isolation and protection of mission-critical systems. As a result, NASA was among the first federal agencies to implement the use of cutting-edge security techniques, including the use of carefully constructed decoy systems (often known as "honeypots") to divert hackers and other intruders away from sensitive operational systems, thus reducing incidences of man-made system outages or disruptions.[19]

[18] *Integration of Security* (NASA OSPP Presentation), October 5, 2005, http://www.hq.nasa.gov/office/ospp/documents/integration-security.ppt
[19] *Wartime CIOs Alter Security Strategies*, Computerworld, April 8, 2002, http://www.computerworld.com/securitytopics/security/story/0,10801,69936,00.html

NASA and Telecommuting

Telecommuting (sometimes referred to in the government as telework) is a facet of an agency's COOP strategy that has met with varying rates of success across the government. OPM has been working with FEMA over the past two years to emphasize telecommuting as a critical component of an agency's COOP plan. Federal COOP architects feel that if facilities are disrupted in the metro Washington DC area, that the ability for employees to work from home in Virginia, Maryland, and surrounding areas will greatly enable agencies to continue a vast majority of operations. However, certain federal agencies (including NASA) have been slower to adopt telecommuting policies and procedures than others, and in certain cases, the Appropriations Committees of Congress have stepped in to provide financial incentives to the slow adopters.

In this fiscal year's *Science, State, Justice, Commerce, and Related Agencies Appropriations Act*, Congress specified that NASA is required to certify as of January 15, 2006 that telecommuting opportunities have been made available to 100 percent of its eligible workforces, or forego five million dollars in funding. Additionally, NASA was ordered to designate an agency "Telework Coordinator" to be responsible for overseeing the implementation and operations of telecommuting programs, and serve as a point of contact on such programs for the Congress.[20] Congress's telecommuting adoption incentive is one that could result in lower total costs of ownership for agencies. A telecommuting system that is developed and implemented earlier in the evolution of an agency's IT architecture (e.g., concurrently with functions such as IT security) can ensure more seamless integration of systems, lower maintenance and upgrade costs, and higher availability of critical data.

NASA Headquarters

NASA's headquarters facility is currently recompeting its COOP services contract, and in August 2005 issued a solicitation for integrated IT systems engineering and operations and related management support services to all mission directorates and mission support offices at NASA Headquarters. The contract is known as Headquarters Information Technology Support Services (HITSS). FSI estimates that an award will be made in April 2006, and is currently valued at approximately $150 million over the life of the five-year contract.

Under the HITSS contract, NASA is seeking a third-party IT provider to fulfill the following set of eight general IT requirements:

1. Application Software and Multimedia Development
2. Software integration
3. Web Development
4. IT Security
5. Systems engineering and integration
6. Computer operations
7. Database administration
8. Configuration management

In addition, the HITSS contract includes to two COOP-specific requirements (which map to OSPP's mission, as described above). These include:

[20] Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006 (H.R.2862), November 22, 2005.

9. *Emergency preparedness*
10. *Continuity of Operations planning, preparation and testing*

The incumbent vendor currently providing these services to NASA is Science Applications International Corporation (SAIC), which has received approximately $206 million in task order business since receiving the original award in May 2000.[21]

Marshall Space Flight Center

Regarding COOP planning at other key NASA facilities, in April 2005 NASA's George C. Marshall Space Flight Center (MSFC) in Huntsville, Alabama, issued its own solicitation for disaster recovery services and facilities through its prime IT systems contractor, Arcata Associates. On June 21, 2005, the subcontract was awarded to SunGard Recovery Services, a company that also serves many COOP customers in the state government arena. The contract was a new solicitation for MSFC and was for one base year (beginning July 1, 2005) with three option periods (ending December 31, 2008).[22]

NASA's MSFC has designed a COOP plan that is applicable to all personnel maintaining the data processing systems for both its mainframe environment (also known as the NASA Data Center, or NDS) and its Integrated Financial Management (IFM) platform. NASA has chartered COOP providers Arcata and SunGard to implement a continuity system that establishes and maintains computing operations at a backup facility, or "Hot Site". If the disruption or outage is longer in duration, the COOP procedures provide for establishment of an alternate computing facility, or "Cold Site", at NASA's Johnson Space Center (JSC) in Houston, Texas.

Under MSFC's COOP plan, the NDC is responsible for the recovery of the Production Operating Systems and Communications Network that comprise the programmatic and administrative framework of the NDC. Once the Operating System is operational at the Hot Site, the NDC then proceeds to the next step of the continuity plan by working with users to recover their applications. SunGard provides operational labor to support COOP testing, as well as tape backups of data using Storage Technology's 9840 model Tape Media.

Two additional requirements for SunGard as NASA MSFC's COOP provider were specified as:

1. Provide one 96-hour COOP test each year for IBM Enterprise Server users and emergency recovery facilities for a period not to exceed six weeks.
2. Provide two 72-hour disaster recovery tests each year for Integrated Financial Management (IFM) platform users and emergency recovery facilities for a period not to exceed six weeks.[23]

Goddard Space Flight Center

NASA's Goddard Space Flight Center (GSFC) in Greenbelt, MD has addressed its own COOP preparation by recently taking steps to expand its distributed storage architecture, thus increasing the availability of key mission-related data in the event of a

[21] FedSources Contracts Database, FSI #FSI0015217
[22] FedSources Contracts Database, FSI #FSI0019350
[23] Ibid.

disruption. In 2004, NASA GSFC solicited information about potential sources for mass data storage and distribution systems for its Solar Dynamics Observatory (SDO) Project at GSFC. The system components required for the distributed storage project included the following:

1. A 42 terabyte fault tolerant redundant array of independent disks (RAID) system capable of storing files created from a continuous 150Mbps data stream
2. A system able to send data, over networks, to three remote "hot sites" at data rates of 72 Mbps, 55 Mbps and 2Mbps
3. Data within the system must be made continuously available for a minimum of five years

While storage solution firm Network Appliance had indicated that it would be open to bidding on the project, it was announced in June 2005 that GSFC's storage infrastructure requirements were ultimately sought under NASA's Scientific & Engineering Workstation Procurement (SEWP) umbrella contract, which is served by a group of prime contractors, including IBM, HP, Northrop Grumman, Unisys, DLT and others.[24]

It should be noted that NASA's GSFC COOP storage requirement of 42 terabytes is exactly twice the size of the facility contracted by DHS's Bureau of Customs and Border protection. This discrepancy is due in large part to the size of the files (*e.g.,* complex, high resolution images and video) that NASA stores and maintains, as opposed to primarily data files and messages in the case of DHS's CBP.

Ames Research Center

In November 2005, NASA's Ames Research Center in Mountain View, California announced that it is seeking to procure services to "support the efficient operation, high-impact utilization, and continual enhancement of NASA supercomputing resources to meet the growing, agency-wide requirements for large-scale computational modeling, simulation, and analysis, to support scientific and engineering excellence in NASA missions." Part of these services includes ensuring the security and availability of data for Ames' NASA Advanced Supercomputing (NAS) facility. Some of these COOP-related services Ames requires under this new contract include:

- Supercomputing and Storage Systems
- Networking and Communications
- Facility Operations
- NASA-Wide Architecture Support
- Program Management[25]

The contract, known as the NASA Supercomputing Support Services (NS3 contract), due to be awarded in February 2007, will support the NAS facility, its high-performance computing (HPC) projects, and its NASA-wide networking infrastructure. This contract may also support COOP and other IT services needs at other NASA HPC facilities. Through this contract, NASA is seeking to transform its multi-facility supercomputing resources into a unified, strategically managed capability for NAS.

[24] FedSources Contracts Database, FSI #FSI0011834
[25] FedSources Contracts Database, FSI #FSI0023868

Incumbent contractor Advanced Management Technology (AMT) held the previous IT services contract with Ames, and was awarded approximately $50 million in task orders over to the two-year contract.[26]

Conclusions

As the US' space agency, NASA has been responsible for developing a range of leading-edge technologies that have allowed it to both explore space and push back the boundaries of science at home. The complexity of the manned and unmanned spacecrafts NASA deploys makes the need for a continuously available IT infrastructure and services paramount, as a major command center disruption on Earth during a Space Shuttle mission could prove disastrous. As a result, NASA has taken a distributed approach to COOP planning and execution, with each major installation nationwide given the authority to contract and acquire the COOP facilities and services it needs. At the same time, NASA HQ is working to coordinate the agency-wide effort, allowing it to leverage the advantages of both centralization and decentralization, in coordination with industry subject matter experts, to keep its COOP plan adaptable moving into the future.

Recommendations

Based upon the findings in the case study above, FedSources offers the following recommendations for COOP professionals:

1. Delaying the adoption of an IT-enabled and organization-wide policy such as telecommuting brings the risk of increased administrative and contract management costs later. Developing a telecommuting system concurrently with other key architectural components, such as IT security, allows organizations (and their systems integrators) to create a system of seamlessly integrated IT components. Reducing system complexity along with the number of back-office processes is a way for agencies to potentially decrease system downtime, reduce maintenance costs, increase availability of data, and decrease total cost of ownership (TCO).

2. In a decentralized organization (such as NASA) there is a risk of higher agency-wide administrative costs if COOP documentation and other key files are kept dispersed rather than coordinated at a central location. In the area of federal cyber-security policy, FISMA has demonstrated that increased regulation compliance and granularity of documentation will likely become the standard in the cases of COOP and telecommuting as well. In the event of an audit, an organization can see administrative expenses (and even potential fines) increase significantly if it does not adopt a disciplined document and records management approach agency-wide.

[26] Ibid.

Internal Revenue Service

FY06 Total Appropriated Budget: $10.7 billion	
IT Requested Budget, FY06: $841.0 million	IT Requested Budget, FY07: $808.7 million
Employees (US): 91,785	Employees (Total WW): 92,609
Chief Information Officer: Mr. W. Todd Grams	

Introduction

Among the President's key executive-level missions for fiscal year 2006 has been deficit reduction. As a result, the US Treasury Department's Internal Revenue Service, which collects more than $2 trillion in revenue and processes more than 227 million returns annually, has been under increasing pressure to simultaneously increase revenues and decrease fraud, abuse, and outstanding tax payments.[27] With an increasing number of tax returns being filed electronically and with back-end systems being constantly upgraded to meet increasing data volume and tightening federal regulations, objectives such as those above can only be accomplished through careful data collection and analysis. However, the best collection and analysis methods are only effective if the data is kept both secure and available. To highlight the real-world impact of effective continuity planning at IRS, the agency recently estimated that lost interest revenue alone could total approximately $264.1 million if the Electronic Federal Tax Payment System was unable to collect taxes for 3 months.[28]

To this end, as the keystone agency within the Treasury Department, the Internal Revenue Service (IRS) has devoted additional time and resources over the past year to its COOP planning efforts. According to the IRS's strategic plan (2005-2009), the IRS will implement disaster recovery capability for computing center assets and disaster recovery plans for all critical infrastructure assets in accordance with business performance expectations. Additionally, the plan states that the IRS will continue efforts to apply adequate security protections and business continuity plans for all mission-critical and business-essential processes, facilities, and assets. Finally, the agency has pledged to develop a business recovery plan and identify alternative locations and sources to complete critical work processes, covering employees, equipment, and shelter for the recovery period.[29]

The IRS's department responsible for COOP planning and execution is its Mission Assurance and Security Services (MA&SS) group, based in New Carrollton, Maryland. The MA&SS group's mission is to assist all IRS operating divisions in ensuring the security of IRS employees, facilities and information technology. (One examples of an IT services firm which has served as a contractor to MA&SS in the past has been Booz Allen Hamilton.)

---

[27] http://www.irs.gov/newsroom/article/0,,id=150358,00.html
[28] http://www.ustreas.gov/tigta/auditreports/2003reports/200320026fr.html
[29] *IRS Strategic Plan, 2005-2009*, http://www.irs.gov/pub/irs-utl/strategic_plan_05-09.pdf

The IRS's MA&SS group's mission today includes the following areas:

1. Information Technology security
2. Physical security
3. Incident management
4. Personnel security
5. Modernization security
6. *Emergency management (incl. COOP; formerly known as 'Enterprise Resilience & Critical Infrastructure Protection')*

Responding to Today's Challenges

The IRS's enterprise-wide COOP challenge involves protecting and ensuring the availability of the following:

- Nine main campuses (which receive tax returns from filers worldwide)
- More than 700 field offices
- Three primary computing centers (*e.g.,* Memphis, Tennessee)
  - Note: Two of these computing centers were affected by the East Coast blackouts of Summer 2003
- 16 mainframe and 900 mid-range computer systems[30]

The IRS's MA&SS (then "Mission Assurance") group finalized an upgraded agency COOP plan immediately following the September 11th attacks based on Federal Preparedness Circular 65 and conducted a major test of the system in August 2002. Following this test, the IRS conducted a significant revision of its COOP plan in spring 2003, and in 2004 created and distributed business continuity templates to all IRS field offices.[31]

An evaluation report following the 2002 COOP test, written by MITRE Corporation of McLean, Virginia, cited the following:

- The Treasury and its Bureaus have developed and established plans that include policies and procedures to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disasters. The plans will be periodically tested and updated to reflect that the changes made to hardware, software, and operational readiness are current.

- Treasury Offices and Bureaus shall:
  - Update their respective COOP and Continuity of Government (COG) plans on at least an annual basis to ensure that the policies and procedures adequately address new and existing critical assets
  - Conduct business impact assessments for critical cyber and physical assets
  - Participate in Treasury-directed continuity of operations exercises
  - Implement and maintain incident or intrusion monitoring and detection capabilities for their respective critical infrastructures[32]

---

[30] *A New Organizational Model: Mission Assurance at the Internal Revenue Service*, February 2004, www.dod-map.msiac.dmso.mil/.../MASI/Carol%20Stender-Larkin_ Mission%20Assurance%20Summit_02092004.ppt

[31] Ibid.

[32] www.mitre.org/work/tech_papers/ tech_papers_03/talley_irs/appendix_b.pdf

While it has made significant strides in its COOP initiatives, the Government Accountability Office (GAO) recently concluded in a report that the IRS had fallen short in effectively implementing certain information security controls relating to physical security, segregation of duties, and service continuity at its Washington DC-based facilities. Specifically, the GAO found that weaknesses in service continuity and business resumption plans increase the risk that the IRS's assets will be inadequately protected and controlled to ensure the continuity of operations when unexpected interruptions occur. Further, the report cited that IRS has implemented some environmental controls designed to protect computing resources and personnel, and also has a program for periodic testing of COOP plans. However, while the IRS has put programs in place to help address the COOP needs of its legacy mainframe infrastructure, the report found that the IRS's disaster recovery and business resumption plans did not yet include procedures for the department's Unix and Windows computing systems.[33]

In addition, a February 2003 memo from the IRS Inspector General (IG) to the CIO highlighted the fact that unauthorized and unencrypted wireless devices were detected within the IRS's COOP infrastructure. While wireless networking had been permitted by the IG as a way for selected agency officials to access IT resources during a major disruption, the wireless devices currently implemented as part of the COOP plan introduced a higher than acceptable level of risk to the IRS.[34]

The above criticisms of the IRS's COOP planning and capacity for handling a major IT system-level outage come at a time when the agency is undertaking a significant expansion of its computing infrastructure. During the FY06 Appropriations cycle, the IRS received $199 million earmarked for its "Business Systems Modernization Program". This funding level the IRS received was equivalent to the President's budget request made to Congress in February 2005 and remains available to the IRS's CIO until September 30, 2008. The funds are to be used for the capital asset acquisition of IT systems, including not merely hardware (*e.g.,* servers, PCs) but also management, operations, and other professional services, including COOP planning.[35]

Conclusions

As the primary conduit into the United States' treasury, the Internal Revenue Service must maintain a highly mission-critical and available infrastructure nationwide. To accomplish this, the department has reorganized internally to create an integrated Mission Assurance group, and has leveraged industry expert firms in the planning, evaluation, and execution phases of its enterprise security and COOP planning efforts. Moving forward, the IRS has demonstrated that it still has several IT challenges to address in areas including client-server infrastructure management and wireless network security. However, the IRS's COOP strategy, based on FPC 65 and the latest FEMA guidance, has been designed as a continuously testable and upgradeable system which will allow the agency to respond to new challenges by incorporating new technologies.

---

[33] *Internal Revenue Service Needs to Remedy Serious Weaknesses over Taxpayer and Bank Secrecy Act Data* (GAO-05-482) , April 2005, http://www.gao.gov/new.items/d05482.pdf

[34] www.ustreas.gov/tigta/auditreports/ 2003reports/200320056fr.html

[35] *Transportation, Treasury, Housing and Urban Development, the Judiciary, the District of Columbia, and Independent Agencies Appropriations Act, 2006* (H.R.3058), November 30, 2005.

Recommendations

Based upon the findings in the case study above, FedSources offers the following recommendations for COOP professionals:

1. Organizations such as the IRS that have unique and stringent up-time requirements (particularly between January and April each year) need to mitigate risk by evaluating their threat environment from all possible perspectives. For example, based on each geographic location and time of year, what are the greatest threats to IT continuity and data availability overall, *e.g.*: extreme weather, loss of power, or outside malicious attack? Only by taking a holistic approach to COOP planning, including one that integrates availability policy with IT security practices, can agencies like the IRS maintain the up-time required to process 227 million returns per year and avoid millions in lost revenues.

2. The IRS's centralized Mission Assurance and Security Services (MA&SS) group allows the agency to leverage best practices (*e.g.,* FEMA's newest COOP templates) by maintaining the COOP planning and updating function within one group at one location. This centralized management structure provides for more streamlined documentation and auditing of COOP activities, thus allowing agencies like the IRS with its 700 field offices to benefit from a centralized, agency-wide, FPC 65-compliant COOP architecture with lower management, administrative, and operational costs across the enterprise.

Appendix: Summary of Key COOP Policy Directives – Federal Level

Contents

Key Policy Directives and Reports

1. *National Infrastructure Protection Plan (Draft v2.0)*
   http://www.ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf
2. *DHS Intelligence Enterprise Strategic Plan*
   http://www.fas.org/irp/agency/dhs/stratplan.pdf
3. *Department of Homeland Security National Response Plan*
   http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf
4. *Federal Preparedness Circular 65: Federal Executive Branch Continuity of Operations*
   http://www.fema.gov/onsc/docs/fpc_65.pdf
5. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*
   http://www.fas.org/irp/offdocs/nspd/hspd-7.html
6. *The National Strategy to Secure Cyberspace*
   http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
7. *Homeland Security Presidential Directive 5: Management of Domestic Incidents*
   http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html
8. *Presidential Decision Directive 67: Enduring Constitutional Government and Continuity of Government Operations*
   http://www.fas.org/irp/offdocs/pdd/pdd-67.htm
9. *Presidential Decision Directive 63: Critical Infrastructure Protection*
   http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
10. *OMB Circular A-130: Management of Federal Information Resources*
    http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Proposed Legislation

11. *Department of Homeland Security Reform Act of 2005*
    http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.4009:
12. *Continuity of Operations Demonstration Project Act*
    http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4797:

Key Policy Directives and Reports

1. *National Infrastructure Protection Plan (NIPP) (Draft v2.0)*, Updated draft released for comment January 20, 2006

Summary: The purpose of this Plan is to outline, using a risk-management based framework, a prioritized plan for each federal agency to work together, under the guidance of DHS and FEMA, to protect the US's Critical Infrastructure and Key Resources (CI/KR) in case of a terrorist attack. Note: This document replaces the *Interim NIPP,* released in February 2005, and *NIPP v1.0*, released for comment November 2005

- The Plan, created in accordance with the policy directives established in HSPD-7 (see below), delineates the specific roles and responsibilities for each security partner (*i.e.,* Executive Branch agency) when carrying out their infrastructure protection activities, while maintaining a flat organizational structure under which each agency retains control of its own jurisdiction.

- Of the 17 key infrastructure areas, or CI/KR sectors, identified in the Plan, DHS is responsible for the *Information Technology* and *Telecommunications* sectors. Looking forward, the Plan is also intended to outline a unifying structure for the integration of both current and future plans for the protection of the nation's Critical Infrastructure and Key Resources.

- For full text: http://www.ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf

---

2. *DHS Intelligence Enterprise Strategic Plan,* Issued January 31, 2006

Summary: This Plan was created by the Department of Homeland Security to articulate its role regarding data security and protection to the US intelligence community, including a new strategic plan for homeland security intelligence and a management directive organizing DHS's intelligence activity.

- The Plan is constructed as a mission statement for DHS intelligence activities across the federal government, outlining seven top-level goals and citing specific objectives within each. The goals range from information sharing and knowledge management to providing analysis and warning functions.
- One specific goal in the Plan outlines the role of COOP in DHS's mission:
    - Mitigation, Prevention, and Readiness: DHS will focus on mitigating threats and preventing attacks against the Homeland, particularly the systems, facilities, and individuals protected by the DHS Stakeholder Community.
    - DHS will act as the Lead the Homeland Security Intelligence Community to support Continuity of Operations (COOP), Continuity of Government (COG) and National Special Security Events (NSSEs) and other special events, emerging incidents, and exercises.
- For full text: http://www.fas.org/irp/agency/dhs/stratplan.pdf

3. *Department of Homeland Security National Response Plan* (NRP), Issued December 2004

Summary: Created in response to HSPD-5 (see below), the purpose of the NRP is to establish a comprehensive, nationwide, all-hazards approach to domestic incident management system across a range of activities including prevention, preparedness, response, and disaster recovery for information and data systems. Note: This document replaces the *Interim NRP,* released in December 2003.

- The NRP's Communication Emergency Support Plan (ESF #2), coordinated by DHS's Information Analysis and Infrastructure Protection Directorate (IAIP), is responsible for coordination with the telecommunications industry; restoration and repair of telecommunications infrastructure; and protection, restoration, and sustainment of national cyber and information technology resources.
- The National Infrastructure Coordinating Center (NICC), managed by DHS IAIP, is chartered with monitoring the nation's critical infrastructure on a constant basis. In the event of an incident, the NICC is to provide a coordinating vehicle to share information with all government entities. Additionally, under the plan agency CIOs are asked to make COOP staff available to the Homeland Security Operations Center (HSOC).
- For full text: http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf

---

4. *Federal Preparedness Circular 65: Federal Executive Branch Continuity of Operations* (FPC 65), First issued July 26, 1999; Updated version issued July 2, 2004

Summary: The purpose of this circular was to provide specific guidance to all federal agencies and departments for development of viable contingency plans for Continuity of Operations (COOP), including details on what a viable plan must include. Note: The 2004 version of FPC 65 replaces the prior version, in addition to FPCs 66 and 67.

- In the original circular, all federal agency heads were required to appoint a COOP program point of contact and develop agency continuity plans (in coordination with FEMA), which were required to include the following sections: Plans and Procedures, Identification of Essential Elements, Delegations of Authority, Orders of Succession, Alternate Facilities, Interoperable Communications, Vital Records and Databases, Tests, Training, and Exercises.
- The 2004 version includes updated, post-9/11 procedures, and a *Reconstitution Annex* with directions for agencies to develop plans for returning to facilities after a threat has passed.
- For full text: http://www.fema.gov/onsc/docs/fpc_65.pdf

5. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7), Issued December 17, 2003

Summary: This Directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. It forms the policy for the *National Infrastructure Protection Plan (NIPP)* (see above).

- The Directive establishes the Critical Infrastructure Protection (CIP) Policy Coordinating Committee, which was chartered to advise DHS on interagency policy related to cyber and physical infrastructure protection. The Secretary of DHS will facilitate collaboration and information sharing between and among federal departments and agencies, state and local governments, the private sector, academia, and international organizations.

- The Office of Science and Technology Policy, in coordination with DHS, is tasked with coordinating interagency research and development (*e.g.,* security standards development) to enhance the protection of critical infrastructure and key resources.

- For full text: http://www.fas.org/irp/offdocs/nspd/hspd-7.html

---

6. *The National Strategy to Secure Cyberspace*, Draft released for comment September 17, 2002; Final Draft issued February 14, 2003

Summary: Created as the IT and data networking-specific companion report to the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (also Feb. 2003), the purpose of this strategy report is to outline a prioritized plan – with the private sector as a key component – to help prevent cyber attacks against America's critical infrastructures, reduce national vulnerability to cyber attacks, and minimize damage and recovery times from cyber attacks.

- The report identifies "public-private engagement" as being a key component to critical data network infrastructure projection, with IT security and continuity software and hardware firms helping to address awareness, training, technological improvements, vulnerability remediation, and recovery operations. Note: The report offers recommendations (*not* policy mandates) to industry, academia, and individual users of technology for securing their own IT systems.

- The report calls for the creation of a National Cyberspace Security Response System (NCSRS), a public-private partnership program coordinated by DHS for managing incidents of national significance; promoting continuity in government systems and private sector infrastructures. Note: The NCSRS' role was updated in 2004 by the NRP to be an advisory group to the Interagency Incident Management Group (IIMG).

- For full text: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

7. *Homeland Security Presidential Directive 5: Management of Domestic Incidents (HSPD-5)*, Issued February 28, 2003

Summary: The first COOP-specific Presidential Directive following the events of 9/11, the purpose of this Directive is to establish a single, comprehensive national incident management system to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters and other emergencies, including critical IT infrastructure protection.

- The directive establishes a National Incident Management System (NIMS), which became mandatory for all federal departments and agencies starting in FY 2005. (See *DHS National Response Plan, December 2004,* above.) The directive outlined plans for interoperability and compatibility among federal, state, and local governments to effectively and efficiently together prepare for, respond to, and recover from domestic incidents, with DHS as top-level coordinator.

- The directive abolished the President's Critical Infrastructure Protection Board, but this was replaced with the Critical Infrastructure Protection (CIP) Policy Coordinating Committee of the National Infrastructure Advisory Council (NIAC), administered under DHS, in December 2003.

- For full text: http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html

---

8. *Presidential Decision Directive 67: Enduring Constitutional Government and Continuity of Government Operations* (PDD NSC-67), Issued October 21, 1998

Summary: The purpose of this Directive is to explain to agencies the roles of continuity of operations (COOP) planning to ensure survival of a constitutional form of government and the continuity of essential federal functions, including information systems.

- Building on the efforts of OMB Circular A-130 (see below), this Directive required federal agencies to develop COOP plans for essential operations. These COOP plans were viewed as a unifying concept not to replace existing plans but, instead, to be superimposed if and when a problem threatens a serious disruption of agency operations.

- In response to this Directive, many federal Executive Branch Secretaries formed task forces of representatives from throughout their agencies who were familiar with government IT contingency plans. The plans identified those requirements necessary to support the primary functions of the agency, such as emergency communications, establishing a chain of command, and delegation of authority.

- For summary: http://www.fas.org/irp/offdocs/pdd/pdd-67.htm

9. *Presidential Decision Directive 63: Critical Infrastructure Protection* (PDD NSC-63), Issued May 22, 1998

Summary: The purpose of this directive is to clearly assign roles and responsibilities within the government for ensuring the continuity of all aspects of the nation's infrastructure (including IT, telephony, and physical infrastructure.)

- The directive created a National Infrastructure Protection Center (NIPC) located within the FBI. The NIPC was chartered with providing a national focal point for gathering information on threats to IT infrastructure, as well as providing the principal means of facilitating and coordinating the government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts.
- The directive also created a Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce. (*Note*: In February 2003, DHS IAIP absorbed the NIPC and CIAO programs.)
- For full text: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

---

10. *OMB Circular A-130: Management of Federal Information Resources* (OMB A-130), Issued February 8, 1996

Summary: This circular, which forms the bedrock of modern federal COOP policy, establishes policy for the overall management of federal information resources. Regarding investments required for data recovery, the circular states that federal agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss of the information.

- The circular establishes that agencies must develop and adhere to an Enterprise Architecture (EA) consisting of information systems that facilitate secure interoperability, application portability, and scalability of applications across networks of heterogeneous hardware, software, and telecommunications platforms.
- The circular further establishes that agency EA plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. These recovery plans must involve automatic recovery and backup procedures that are to be tested on a periodic basis.
- For full text: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Proposed Legislation

11. *Department of Homeland Security Reform Act of 2005* (HR 4009), Introduced October 6, 2005, Status: Under review by House Transportation & Infrastructure Subcommittee

Summary: Among the purposes of this Act is to create a Chief Intelligence Officer within DHS, chartered with creating a continuity of operations (COOP) plan that assures uninterrupted intelligence analysis, collection, and related functions during emergencies. Due to its nature, this intelligence data needs to be kept not merely available but highly secure.

- The Act establishes an Office of Intelligence Analysis (OIA) within DHS, led by a Chief Intelligence Officer (a Presidential Appointment (PA) post carrying a Senior Executive Service (ES) Level II pay grade). The Chief Intelligence Officer is chartered with creating, in consultation with the Assistant Secretary for Physical Infrastructure Security, a continuity of operations (COOP) plan for the nation's intelligence infrastructure. The COOP plan is to assure uninterrupted intelligence analysis, collection, and related functions during a wide range of potential disruptions, including localized acts of nature, accidents, and technological or attack-related emergencies.

- The COOP plan is to include procedures governing the improvisation or emergency acquisition of vital resources necessary for the performance of government operations and the capability to relocate essential personnel and functions to and to sustain the performance of the operations of the OIA at an alternate work site until normal operations can be resumed (*i.e.,* implement a telecommuting solution).

- For full text: http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.4009:

---

12. *Continuity of Operations Demonstration Project Act* (HR 4797), Introduced July 9, 2004, Status: Introductory remarks submitted by House Government Reform Committee

Summary: The purpose of this Act is to provide organizational structure and funding for a demonstration project to highlight the ability of a federal COOP plan. The Act defines for the first time a 30-day minimum requirement for any viable continuity plan to provide full and secure remote access to government networks.

- Under the Act, the U.S. Chief Human Capital Officers Council (CHCOC) is chartered with establishing a COOP demonstration project, under which a representative range of government services and operations shall be performed under circumstances simulating a situation in which Federal employees are, as a result of a sudden and unexpected contingency, required to work from home for more than 30 days, yet are able to access all technologies and systems required to execute their duties.

- The goals of the Act include determining which private sector technologies are needed for federal employees to work under such constraints, and enhancing the government's ability to manage personnel and operations activities.

- For full text: http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4797: