

Department-wide Systems and Capital Investment Program

Mission:

To modernize business processes and increase efficiencies throughout the Department of Treasury through technology investments.

Program Summary

(Dollars in Thousands)

Appropriations	FY 2005	FY 2006	FY 2007		
	Enacted	Enacted	President's Budget	Change	% Change
Department-wide Systems & Capital Invest. Program	\$32,002	\$24,168	\$34,032	\$9,864	40.8%
Treasury Foreign Intelligence Network (TFIN)	0	5,940	21,200	15,260	256.9%
Treasury Secure Data Network (TSDN)	0	2,772	4,003	1,231	44.4%
OFAC Enterprise Content Management	0	0	627	627	0.0%
Critical Infrastructure Protection (Fin. Inst.)	5,754	5,742	2,093	(3,649)	-63.5%
Treasury Back-up Disaster Recovery Capacity	1,732	1,729	1,656	(73)	-4.2%
Cyber Security	2,540	2,281	2,244	(37)	-1.6%
E-Government Initiatives	2,740	2,734	2,209	(525)	-19.2%
Integrated Wireless Network	1,488	1,485	0	(1,485)	-100.0%
Enterprise Architecture	397	396	0	(396)	-100.0%
HR Connect	15,367	0	0	0	0.0%
Appliance-Based Computer Security	1,488	0	0	0	0.0%
Certificate-Based Internet Security	496	0	0	0	0.0%
Defense Messaging System	0	495	0	(495)	-100.0%
Documents Management	0	594	0	(594)	-100.0%
Subtotal, Dept.-wide System & Capital Investments Program	\$32,002	\$24,168	\$34,032	\$9,864	40.8%
Total Operating Level	\$32,002	\$24,168	\$34,032	\$9,864	40.8%

Overview

The Department-wide Systems and Capital Investments Program (DSCIP) account is authorized to be used by or on behalf of Treasury bureaus, at the Secretary's discretion, to modernize business processes and increase efficiency through technology investments. Continuing investments include the Treasury Foreign Intelligence Network, Treasury Secure Data Network, Critical Infrastructure Protection, Back-up Disaster Recovery Capacity, Cyber Security, and various E-Government initiatives.

Treasury has made significant progress in key initiatives under the DSCIP program. In FY 2005, Treasury:

- Completed investments in HR Connect,
- Completed assessment and evaluation of the Department's critical cyber and physical assets and key resources, and
- Improved Federal Information Security Management Act (FISMA) performance.

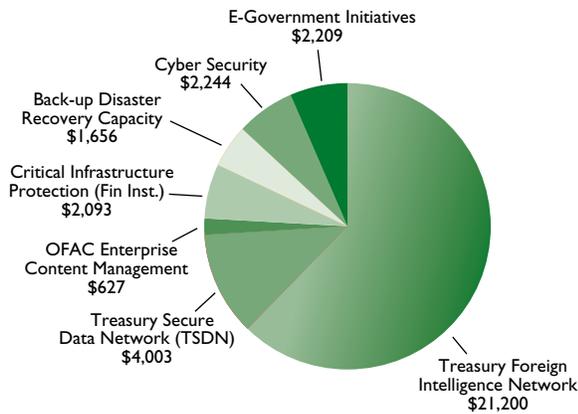
In FY 2006, Treasury will invest in the Treasury Foreign Intelligence Network, Treasury Secure Data Network, Defense Messaging System and Documents Management, while continuing investments in Critical Infrastructure Protection (CIP), E-Government, Treasury Back-up Disaster Recovery, Integrated Wireless Network, Cyber Security and Enterprise Architecture. These capital investment projects, critical to Treasury's ability to

efficiently carry out its mission, will continue in FY 2007. Funding is requested in FY 2007 to plan for the development of an Enterprise Content Management system for the Office of Foreign Assets Control, as part of the overall Department effort to develop Treasury-wide document management systems.

The FY 2007 request for Department-wide Systems and Capital Investment Program is \$34,032,000, an increase of \$9,864,000 above the FY 2006 enacted level.

DSCIP Funding by Program

(Dollars in Thousands)



Performance Highlights

Treasury has made significant progress on key initiatives managed through the DSCIP program. Highlights of these accomplishments include:

Critical Infrastructure Protection (CIP): Homeland Security Presidential Directive 7 (HSPD-7) requires that federal agencies identify, prioritize and determine the interdependencies of critical assets in order to provide an appropriate level of cyber and physical asset protection. Treasury completed the Project Matrix Refresh effort, an assessment and evaluation of the Department’s critical cyber and physical assets and key resources. This initiative, one of the Department’s “Proud To Be” milestones under the President’s Management Agenda, assists Treasury in its emergency preparedness efforts and disaster recovery planning. Completion of

Project Matrix Refresh also enables the Department of Homeland Security to address assets and key resources across the federal government that impact U.S. national security.

Presidential E-Government Initiatives: Treasury is fully participating in 17 of the 25 E-Government initiatives and four of the six E-Government Lines of Business. Treasury worked diligently with the Managing Partners of the Presidential E-Government Initiatives and completed all required Memoranda of Understanding with other federal agencies by March 30, 2005. By facilitating discussions between Departmental E-Government representatives and the Federal Managing Partners, Treasury-wide coordination has improved and transition activities have begun to identify and eliminate duplicative systems.

Cyber Security: Improvements have been made in Treasury’s Federal Information Security Management Act (FISMA) performance. For example, gains have been made in the number of Treasury systems certified and accredited.

In FY 2005, the Office of Domestic Finance contributed to the Department’s strategic objectives to increase resiliency and protection of the financial system by:

- Increasing the number of protective response planning exercises for critical institutions,
- Continuing to test crisis response of Federal financial regulators,
- Working with the Financial Services Information Sharing and Analysis Center to ensure it has accurate and useful information and that it continues to build membership,
- Working with other sectors on which financial services is interdependent to address vulnerabilities, as well as improving the tools and processes used to communicate with the public and private sectors,
- Monitoring the finalization of rules and implementation of procedures required under

DSCIP Performance by Budget Activity

Budget Activity	Performance Measure	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	
		Actual	Actual	Actual	Target Met?	Target	Target
Department-wide Systems and Capital Investments Program	Increase the quality of information sharing of U.S. financial information between the Federal government and the U.S. financial services sector institutions. (%) (Ot)	67	309	20	✓	10	0
	Increase the reliance of Treasury programs to ensure the effective operation of the U.S. financial system. (% growth) (Ot)	n/a	n/a	n/a	n/a	6	6
	Support and encourage the formation of regional coalitions. (Ot)	n/a	n/a	n/a	n/a	2	2
	Treasury Secure Data Network (TSDN) is within 10 percent of cost and schedule. (%) (E)	n/a	n/a	n/a	n/a	10	10
	Treasury Foreign Intelligence Network (TFIN) is within 10 percent of cost and schedule. (%) (E)	n/a	n/a	n/a	n/a	10	10
	Office of Foreign Assets Control (OFAC) Enterprise Content Management is within 10 percent of cost and schedule. (%) (E)	n/a	n/a	n/a	n/a	10	10

(E) = Efficiency Measure (Oe) = Outcome Measure (Ot) = Output Measure

the Fair and Accurate Credit Transactions Act to ensure consistency with the intent of the statute, and

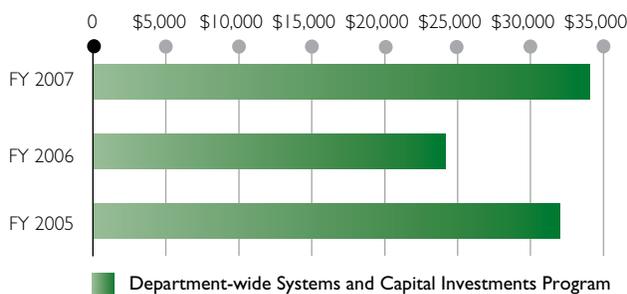
- Discharging Treasury's obligations under Homeland Security Presidential Directive 7.

Source of Funds

The DSCIP request of \$34,032,000 is from direct appropriations.

DSCIP Funding History

(Dollars in Thousands)



FY 2007 Budget Adjustments

FY 2006 Current Estimate

The FY 2006 current estimate of DSCIP appropriations is a total of \$24,168,000 to fund the following investments: Treasury Foreign Intelligence Network (TFIN), Treasury Secure Data Network (TSDN) the Critical Infrastructure Program, E-Government Initiatives, Treasury Back-up Disaster Recovery Capacity, Integrated Wireless Network, Cyber Security, Enterprise Architecture, Defense Messaging System, and Documents Management.

Planned Investments

Treasury Foreign Intelligence Network (TFIN) +21,200,000/0 FTE The Office of Terrorism and Financial Intelligence is responsible for coordinating bureau and policy office intelligence related to terrorist financing and other national security threats related to financial crime. As Treasury's role in supporting the intelligence community and national security directives continues to grow, so does the urgent requirement for a robust, reliable, and secure classified network. TFIN is a Top Secret/Sensitive Compartmented

Information (TS/SCI) system critical to the support of Treasury's national security mission. Current TFIN network equipment and software is unstable and soon will no longer receive technical support from the manufacturer. It has become increasingly difficult for Treasury to exchange information with the intelligence community and other necessary entities.

A system upgrade is needed to address network stability and ensure adequate cyber security capabilities. These enhancements are necessary to bring the operating system and related security measures into line with the rest of the intelligence community. TFIN is the Department's top priority. The FY 2007 request will complete the redesign and modernization of TFIN in FY 2007 and the installation of full back up and recovery capability for TFIN in the second quarter of FY 2008. A redesigned TFIN will fully leverage new technologies and capabilities and include replacement of core servers, terminals, and funding for maintenance. Enhancements include replacement of the secure messaging system, connection to the Defense Messaging System, and an intelligence community-compatible analytical toolset for use by analysts and the watch office.

Treasury Secure Data Network (TSDN) +\$4,003,000 /0 FTE The Treasury Secure Data Network (TSDN) is the computer and network infrastructure that enables the communication and distribution of classified information to over 400 Departmental users. TSDN also provides Treasury users with access to the Secret Internet Protocol Router Network and the Department of Defense classified communications network, which is vital to ensure that the Office of Terrorism and Financial Intelligence, as well as IRS-Criminal Investigations, can communicate effectively with colleagues in the law enforcement and intelligence communities. Currently, most national security cable traffic, classified data, and policy information must be compiled and formulated on stand-alone personal computers and hand-carried to recipients. Full implementation of TSDN will provide staff with the capability to

sort and distribute such information electronically and perform retrospective searches across multiple years of data. In addition, the current system will soon be out-of-date and no longer supported by the manufacturer. Treasury's increasing role in national security drives the greater demand for TSDN seats and services.

Office of Foreign Assets Control (OFAC) Enterprise Content Management +\$627,000/0 FTE Productivity and response time improvements are critical to OFAC's continued success. An analysis of unclassified mission critical OFAC functions determined that OFAC needs an Enterprise Content Management (ECM) case-centric solution to replace its dependence on a document-centric process. Currently case folders are used in virtually every aspect of OFAC's operations, including processing licenses, investigating potential violations, and administering penalties. These folders organize all relevant documents, including correspondence, routing memos, case notes, and checklists. OFAC also needs an automated document or records management system for routing or searching for documents. An ECM solution will allow OFAC to better meet its commitments, manage its records, respond to inquiries from citizens, including Freedom of Information Act requests, and better serve its business and government customers. The FY 2007 request will fund the planning phase for ECM. OFAC will work with the Office of the Chief Information Officer to ensure that OFAC's planning is coordinated with the Department's efforts to plan for document management systems Treasury-wide.

Critical Infrastructure Protection (Financial Institutions) +\$2,093,000/0 FTE Treasury has the lead role in the Homeland Security Presidential Directive 7 (HSPD-7) that protects the U.S. banking and finance sector's critical infrastructure. This funding is requested to decrease the financial sector's susceptibility to terrorist events and natural disasters. An example of HSPD-7 and CIP efforts is the response mechanisms that helped restore financial services in the aftermath

of Hurricane Katrina. Response was much quicker in areas impacted by the storms, as regulatory obstacles like the waiving of certain rules were removed, allowing financial institutions to co-locate in undamaged buildings. Treasury also informed the financial institutions about federal relief payments, policies on the cashing of checks issued by the government, and restoration plans for electricity and telecommunications.

Back-up Disaster Recovery Capacity +\$1,656,000/0 FTE Treasury must maintain and enhance the Department's disaster recovery capabilities. These critical efforts protect many of Treasury's technology systems and provide for the continuity of operations for key Treasury officials and functions in the event of a disaster. This provides for ongoing support for existing servers, software for DO critical services such as email, shared drive and mainframe applications, email archiving and internet access.

Cyber Security +\$2,244,000/0 FTE This program ensures Department-wide compliance with Federal and Treasury security policy, and in particular, with the Federal Information Security Management Act (FISMA). Funding is requested to protect Treasury's security posture by providing adequate policy and compliance reviews, and to improve the Department's FISMA performance and overall cyber security posture. In October 2005, Treasury's Office of Inspector General (OIG) found that Treasury was in substantial non-compliance with FISMA. According to the Congressional scorecard, the Department currently has a grade of "D." Under current conditions, Treasury's risk for catastrophic network intrusion, including exposure of sensitive, collateral classified and intelligence information processed by Treasury systems, could increase. This funding also supports the majority of compliance and oversight activities required by various laws and directives that are enforced by the OIG, Government Accountability Office, and Office of Management and Budget. Funding is requested to prevent non-compliance with the law and regulatory requirements in many potential areas.

E-Government Initiatives +\$2,209,000/0 FTE The Office of the Chief of Information Officer (OCIO) oversees the Department's participation in the Government-wide E-Government initiatives. As provided by the E-Government Act of 2002 and the President's Management Agenda, Treasury receives services from the shared solutions developed within a number of the E-Government Initiatives and Lines of Business. Treasury is currently a partner in 17 of these initiatives and four Lines of Business. OCIO ensures the execution of Memoranda of Understanding with the Managing Partner agencies and commits Treasury to fulfilling its contribution to the initiatives as agreed to with the Managing Partner agencies.

