



DHS Exhibit 300 Public Release BY08 (Form) / Prep - CNDSP Computer Network Service Defense Provider (2008) (Item)

Form Report, printed by: Administrator, System, Feb 12, 2007

OVERVIEW

General Information

1. Date of Submission:	Jan 12, 2007
2. Agency:	Department of Homeland Security
3. Bureau:	Preparedness (PREP)
4. Name of this Capital Asset:	Prep - CNDSP Computer Network Service Defense Provider (2008)
Investment Portfolio:	PREP C&T Home 2008
5. Unique ID:	024-65-01-04-01-9511-00

(For IT investments only, see section 53. For all other, use agency ID system.)

All investments

6. What kind of investment will this be in FY2008? (Please NOTE: Investments moving to O&M ONLY in FY2008, with Planning/Acquisition activities prior to FY2008 should not select O&M. These investments should indicate their current status.)
Acquisition
7. What was the first budget year this investment was submitted to OMB?
FY2007
8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap.
The overarching goal of the Computer Network Defense Service Provider (CNDSP) program is to ensure the efficiency and quality of IT security across the Federal government. The US-CERT is developing a set of Computer Network Defense (CND) performance metrics that have been adapted from the Department of Defense (DOD) 8530 Directive and Instruction for Certification and Accreditation of Computer Network Defense Service Providers (based on the DOD version dated December 2004). CND services are those services considered essential to protecting, defending, and sustaining an agency's computing environment, in addition to conducting appropriate response actions. Such services are often provided by security or network operators but can also be provided and managed by a Computer Security Incident Response Team (CSIRT). The purpose of the federalized metrics is to provide Federal, state, and local government agencies with an assessment tool that to benchmark their incident management capability and/or to improve the Protect, Detect, Response, and Sustainment activities for computer network defense within their agencies.
9. Did the Agency's Executive/Investment Committee approve this request?
Yes
9.a. If "yes," what was the date of this approval?
Apr 16, 2006
10. Did the Project Manager review this Exhibit?
Yes
12. Has the agency developed and/or promoted cost effective, energy-efficient and environmentally sustainable techniques or practices for this project.
Yes
12.a. Will this investment include electronic assets (including computers)?
Yes
12.b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only)
No
12.b.1. If "yes," is an ESPC or UESC being used to help fund this investment?
12.b.2. If "yes," will this investment meet sustainable design principles?
12.b.3. If "yes," is it designed to be 30% more energy efficient than relevant code?
13. Does this investment support one of the PMA initiatives?
Yes
If "yes," select the initiatives that apply:

Human Capital

Yes

Budget Performance Integration	Yes
Financial Performance	No
Expanded E-Government	Yes
Competitive Sourcing	Yes
Faith Based and Community	No
Real Property Asset Management	No
Eliminating Improper Payments	No
Privatization of Military Housing	No
R and D Investment Criteria	No
Housing and Urban Development Management and Performance	No
Broadening Health Insurance Coverage through State Initiatives	No
Right Sized Overseas Presence	No
Coordination of VA and DoD Programs and Systems	No

13.a. Briefly describe how this asset directly supports the identified initiative(s)?

By creating metrics for how CSIRTs should operate and encouraging agencies to adopt organizational planning metrics to mitigate computer attacks, CNDSP helps avoid costs to protect, defend and sustain an agency's computing environment and permits economic/efficient human capital management. CNDSP allows experts to improve program capabilities and achieve expected results, ensuring that proper funding is received by providing standard metrics to mitigate computer attacks and associated training.

14. Does this investment support a program assessed using OMB's Program Assessment Rating Tool (PART)?

Yes

14.a. If "yes," does this investment address a weakness found during the PART review?

Yes

14.b. If "yes," what is the name of the PART program assessed by OMB's Program Assessment Rating Tool?

PREP – Cyber Security

14.c. If "yes," what PART rating did it receive?

Results Not Demonstrated

15. Is this investment for information technology (See section 53 for definition)?

Yes

For information technology investments only:

16. What is the level of the IT Project (per CIO Council's PM Guidance)?

Level 3

17. What project management qualifications does the Project Manager have? (per CIO Council's PM Guidance)

(4) Project manager assigned but qualification status review has not yet started

18. Is this investment identified as "high risk" on the Q4 - FY 2006 agency high risk report (per OMB's 'high risk' memo)?

No

19. Is this a financial management system?

No


19.a. If "yes," does this investment address a FFIA compliance area?

19.a.1. If "yes," which compliance area:

19.a.2. If "no," what does it address?

19.b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52.

20. What is the percentage breakout for the total FY2008 funding request for the following? (This should total 100%)

Area	Percentage	
Hardware	30.00	
Software	30.00	
Services	10.00	
Other	30.00	
Total	100.00	

21. If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities?

N/A

23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?

Yes

SUMMARY OF FUNDING

SUMMARY OF SPENDING FOR PROJECT PHASES (In Millions)

1. Provide the total estimated life-cycle cost for this investment by completing the following table. All amounts represent budget authority in millions, and are rounded to three decimal places. Federal personnel costs should be included only in the row designated "Government FTE Cost," and should be excluded from the amounts shown for "Planning," "Full Acquisition," and "Operation/Maintenance." The total estimated annual cost of the investment is the sum of costs for "Planning," "Full Acquisition," and "Operation/Maintenance." For Federal buildings and facilities, life-cycle costs should include long term energy, environmental, decommissioning, and/or restoration costs. The costs associated with the entire life-cycle of the investment should be included in this report.

All amounts represent Budget Authority

	PY-1 & Earlier	PY	CY	BY
	-2005	2006	2007	2008
Planning:				
Budgetary Resources	0.000	0.123	0.103	0.000
Acquisition:				
Budgetary Resources	0.000	0.136	0.113	0.000
Subtotal:				
Budgetary Resources	0.000	0.259	0.216	0.000
Maintenance:				
Budgetary Resources	0.000	0.014	0.014	0.000
TOTAL, All Stages				
Budgetary Resources	0.000	0.273	0.230	0.000
Government FTE Cost	0.000	0.177	0.175	0.000
# of FTEs	0.00	2.00	1.00	0.00
Total, BR + FTE Cost	0.000	0.450	0.405	0.000

Note: For the cross-agency investments, this table should include all funding (both managing partner and partner agencies).

Government FTE Costs should not be included as part of the TOTAL represented.

2. Will this project require the agency to hire additional FTE's?

No

2.a. If "yes," how many and in what year?

3. If the summary of spending has changed from the FY2007 President's budget request, briefly explain those changes.