1999 Current Fiscal Year Report: Technical Advisory Committee to Develop a Federal Information Processing Standard for the Key Management Infrastructure

Report Run Date: 06/16/2019 03:30:19 PM

1. Department or Agency	2. Fiscal Year
Department of Commerce	1999

3. Committee or Subcommittee	3b. GSA Committee No.
Technical Advisory Committee to Develop a Federal Information Processing Standard for the Key Management Infrastructure	1999

4. Is this New During Fiscal Year?	5. Current Charter	6. Expected Renewal Date	7. Expected Term Date
No	07/16/1998		12/31/1998

8a. Was Terminated During FiscalYear?	8b. Specific Termination Authority	8c. Actual Term Date
Yes	CFO & A/S for Administration, Dept. of Commerce	12/31/1998

9. Agency Recommendation for Next FiscalYear	10a. Legislation Req to Terminate?	10b. Legislation Pending?
Terminate	No	

11. Establishment Authority Agency Authority

12. Specific Establishment Authority	13. Effective Date	14. Commitee Type	14c. Presidential?
Secretary's Decision Memorandum	06/21/1996	Continuing	No

15. Description of Committee Scientific Technical Program Advisory Board

16a. Total Number of Reports 1

16b. Report Date	Report Title
11/30/1998	Requirements for Key Recovery Products

Number of Committee Reports Listed: 1

17a. Open 1 **17b. Closed** 0 **17c. Partially Closed** 0 **Other Activities** 0 **17d. Total** 1

Meetings and Dates

Purpose	Start	End
To finalize the draft FIPS for Cryptographic Key Recovery Systems	11/17/1998	- 11/19/1998

Number of Committee Meetings Listed: 1

	Current FY	Next FY
18a(1). Personnel Pmts to Non-Federal Members	$0.00	$0.00
18a(2). Personnel Pmts to Federal Members	$0.00	$0.00

18a(3). Personnel Pmts to Federal Staff	$25,834.00	$0.00
18a(4). Personnel Pmts to Non-Member Consultants	$0.00	$0.00
18b(1). Travel and Per Diem to Non-Federal Members	$6,652.00	$0.00
18b(2). Travel and Per Diem to Federal Members	$835.00	$0.00
18b(3). Travel and Per Diem to Federal Staff	$1,670.00	$0.00
18b(4). Travel and Per Diem to Non-member Consultants	$0.00	$0.00
18c. Other(rents,user charges, graphics, printing, mail, etc.)	$1,000.00	$0.00
18d. Total	$35,991.00	$0.00
19. Federal Staff Support Years (FTE)	0.30	0.00

20a. How does the Committee accomplish its purpose?

The Committee makes technical recommendations regarding the development of a draft FIPS for Cryptographic Key Recovery Systems which could be incorporated into a Federal Key Management Infrastructure. The Committee focuses on the key recovery services of the Federal Key Management Infrastructure for both stored and communicated information. The Board held its twelfth and final meeting in November 1998 to review the final draft document to be forwarded to the Secretary of Commerce for submission to NIST for development as a FIPS.

20b. How does the Committee balance its membership?

The members, appointed by the Secretary of Commerce, are selected solely on the basis of established technical expertise in cryptography and the implementation of cryptographic systems. Federal government employees may serve as members of the Committee. The Committee membership numbers 18 members appointed for a two-year term. Members are drawn from academia, IT vendors, security-specific product vendors, IT users and other categories of interest.

20c. How frequent and relevant are the Committee Meetings?

The Committee meets at least quarterly at the call of the Chairperson and may hold additional meetings whenever one-third of the members so request in writing. At each meeting, the Committee reviews, discusses and revises the current version of the draft document. The last meeting of the Board was held on November 17-19, 1998 in Orlando, Florida.

20d. Why can't the advice or information this committee provides be obtained elsewhere?

Use of strong cryptography on a widespread basis in the GII requires a supporting infrastructure, including the provision of many services. One important service is key recovery (for keys used for confidentiality). To facilitate provision of key recovery services

for its own use, the government needs an encryption key recovery standard. The standard must be developed by working with those who produce and use cryptographic technologies in the private sector. This Committee, comprised primarily of private sector individuals, will be an important vehicle by which the government gains the benefit of private sector input in developing this standard.

20e. Why is it necessary to close and/or partially closed committee meetings?
N/A

21. Remarks

Designated Federal Officer
Edward J. Roback DFO

Committee Members	Start	End	Occupation	Member Designation
Alexander, Joe	11/21/1996	12/31/1998	Sun Microsystems Computer Corporation	Special Government Employee (SGE) Member
Benaloh, Josh	12/10/1996	12/31/1998	Microsoft Corporation	Special Government Employee (SGE) Member
Carman, David	11/21/1996	12/31/1998	Trusted Information Systems Labs at Network Associates,	Special Government Employee (SGE) Member
Chohkani, Santosh	11/21/1996	12/31/1998	CygnaCom Solutions	Special Government Employee (SGE) Member
Clark, Paul	06/19/1997	12/31/1998	DynCorp	Special Government Employee (SGE) Member
Edwards, John	11/21/1996	12/31/1998	DIGICOM, Inc.	Special Government Employee (SGE) Member
Etzel, Mark	11/21/1996	12/31/1998	Lucent Technologies Bell Laboratories	Special Government Employee (SGE) Member
Franklin, William	11/21/1996	12/31/1998	IBM Corporation	Special Government Employee (SGE) Member
French, Roger	12/10/1996	12/31/1998	COMPAQ/Digital Equipment Corporation	Special Government Employee (SGE) Member
Harkins, Daniel	06/19/1997	12/31/1998	Cisco Systems, Inc.	Special Government Employee (SGE) Member
Hite, Richard	12/18/1996	12/31/1998	VISA International	Special Government Employee (SGE) Member
Housley, Russell	11/21/1996	12/31/1998	SPYRUS, Inc.	Special Government Employee (SGE) Member
Kent, Stephen	11/21/1996	12/31/1998	BBN Systems	Special Government Employee (SGE) Member
Konechy, Ken	12/10/1996	12/31/1998	Rainbow Technologies, Inc.	Special Government Employee (SGE) Member
Lambert, Paul	06/19/1997	12/31/1998	Certicom Corporation	Special Government Employee (SGE) Member
Markowitz, Michael	11/21/1996	12/31/1998	Information Security Corporation	Special Government Employee (SGE) Member
Matyas, Stephen	12/10/1996	12/31/1998	IBM Corporation	Special Government Employee (SGE) Member

Pato, Joe	12/10/1996	12/31/1998	Hewlett-Packard Laboratories	Special Government Employee (SGE) Member

Number of Committee Members Listed: 18

Narrative Description

What are the most significant program outcomes associated with this committee?

	Checked if Applies
Improvements to health or safety	☐
Trust in government	☐
Major policy changes	☐
Advance in scientific research	☐
Effective grant making	☐
Improved service delivery	☐
Increased customer satisfaction	☐
Implementation of laws or regulatory requirements	☐
Other	☐

Outcome Comments

What are the cost savings associated with this committee?

	Checked if Applies
None	☑
Unable to Determine	☐
Under $100,000	☐
$100,000 - $500,000	☐
$500,001 - $1,000,000	☐
$1,000,001 - $5,000,000	☐
$5,000,001 - $10,000,000	☐
Over $10,000,000	☐
Cost Savings Other	☐

Cost Savings Comments

What is the approximate Number of recommendations produced by this committee for the life of the committee?

0

Number of Recommendations Comments

What is the approximate Percentage of these recommendations that have been or will be Fully implemented by the agency?
0%

% of Recommendations Fully Implemented Comments

What is the approximate Percentage of these recommendations that have been or will be Partially implemented by the agency?
0%

% of Recommendations Partially Implemented Comments

Does the agency provide the committee with feedback regarding actions taken to implement recommendations or advice offered?
Yes ☐ No ☐ Not Applicable ☑

Agency Feedback Comments

What other actions has the agency taken as a result of the committee's advice or recommendation?

	Checked if Applies
Reorganized Priorities	☐
Reallocated resources	☐
Issued new regulation	☐
Proposed legislation	☐
Approved grants or other payments	☐
Other	☐

Action Comments

Is the Committee engaged in the review of applications for grants?

No

Grant Review Comments

How is access provided to the information for the Committee's documentation?

	Checked if Applies
Contact DFO	☐
Online Agency Web Site	☐
Online Committee Web Site	☐
Online GSA FACA Web Site	☐
Publications	☐
Other	☐

Access Comments