GAO

Testimony

STATUS OF COMPLIANCE WITH THE COMPUTER
SECURITY ACT OF 1987

STATEMENT OF
HOWARD G. RHILE, ASSOCIATE DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND
MATERIALS
COMMITTEE ON SPACE, SCIENCE AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

136863

043307/136863

GAO CMTE-T-38-8

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to respond to your request for testimony on federal agencies' progress in implementing the Computer Security Act of 1987. As you know, at the request of two Chairmen, we are conducting a three-part effort to determine whether federal agencies are complying with specific requirements and deadlines of the act. My statement today summarizes the results of the first part of our work, federal agencies' compliance with the Act's July 8, 1988 requirements to issue training regulations and identify their computer systems that contain sensitive information. We are also issuing a report today that details the results of this work. With your permission, I would like to place it in the record of this hearing.

Our future work will focus on agencies' compliance with the Act's requirements to establish training programs and security plans for their sensitive systems.

Training Regulation Due By July 8, 1988

With regard to the training regulation due by July 8, 1988, the Office of Personnel Management distributed an interim regulation on this date entitled Training Requirement for the Computer Security Act at a government-sponsored briefing and seminar on implementation of the act. The interim training regulation became effective and was published in the Federal

Register on July 13, 1983. It outlines federal agencies' training
responsibilities under the Act, and points out that training should

   -- stress the vulnerability of computer systems;

   -- be organized around the agency's security policies,
      practices, and procedures; and

   -- be a continuous process.

On July 8, 1988, The National Institute of Standards
Technology, formerly the National Bureau of Standards, also issued
a training document entitled, Computer Security Training
Guidelines. The purpose of these guidelines is to help agencies in
developing and selecting training in computer security awareness
and accepted security practices. The guidelines were prepared in
consultation with the Office of Personnel Management.

Sensitive Computer Systems to be Identified by July 8, 1988

To determine federal agencies' compliance with the Act's
requirement to identify their sensitive systems by July 8, 1988, we
sent a questionnaire to 89 agencies that were not specifically
exempted. Five of these agencies reported that they were not
subject to the Act. After reviewing their reasoning, we agree that
3 of them did not fall under the Act's definition of a federal
agency. A fourth agency reported that it was exempt because it
did not have any federal computer systems as defined by the Act.

2

The fifth agency, the CIA, said it would send us documentation to support its reasoning that it was exempt from the Act.

SEE CHART 1

I would now like to direct your attention to the chart before you. The chart shows the responses to the questionnaires mailed to the remaining 84 federal agencies. I must point out that, as discussed with your office, we did not independently verify the information in the agencies' responses.

In response to our questionnaire as of September 8, 1988

-- 74 agencies or about 88 percent responded that they
   identified all of their sensitive systems. Of these:
   -- 65 agencies reported they had identified their sensitive
      systems as of July 8, 1988.
   -- 9 agencies reported they had identified their sensitive
      systems after July 8, 1988.
-- 6 agencies reported they had not yet identified all their
   sensitive systems. These agencies--Agriculture, Interior,
   VA, FEMA, ICC, and FCC--estimated they would complete
   identification by December 1988. I would like to note that
   Interior told us a few days ago that they had identified
   all their sensitive systems.
-- 4 agencies did not respond to our questionnaire as of
   September 8, 1988--the National Security Council and 3
   legislative agencies, the Congressional Budget Office, the

3

Library of Congress, and the Office of Technology
Assessment. These legislative agencies initially told us
that they were unsure as to whether they were subject to
the Act. They called us a few days ago, however, and have
determined that they are subject to the Act and are taking
action to comply. The National Security Council recently
told us that it had not yet decided whether to respond to
our questionnaire.

Numbers of Sensitive Systems Identified by Federal Agencies
SEE CHART 2

I would now like to direct your attention to the other chart
which I brought with me today. This chart shows the number of
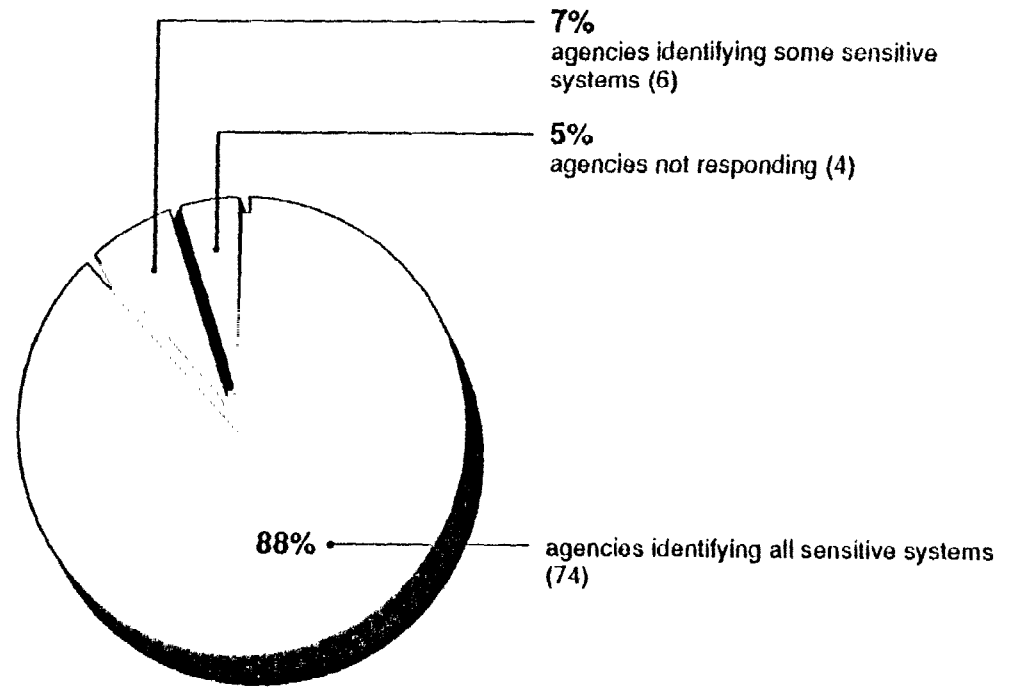sensitive systems identified by federal agencies.

Seventy-two of the 74 agencies that had identified all their
sensitive systems reported the number of sensitive systems they
identified:

-- Navy reported 27,000 systems or about one-half of the
   systems reported;
-- Army reported 12,000 systems, about 23 percent;
-- Air Force reported 10,000 systems or about 19 percent;
-- Other DOD components reported 3,000 systems, 6 percent; and
-- All civilian agencies reported about 1,400 systems or 3
   percent of the total.

In summary then, it appears that federal agencies are attempting to comply with the requirements of the Computer Security Act of 1987. The Office of Personnel Management's training regulation became effective on July 13, 1988, five days after the Act's July 8, 1988 deadline. Based on our questionnaire responses, about 77 percent of the federal agencies had identified their computer systems with sensitive information by the July 8, 1988 deadline. And about 90 percent of the agencies have identified all their sensitive computer systems, as of today.

This concludes my prepared statement, Mr. Chairman. I will be pleased to answer any questions that you or others may have at this time.

Identification of Sensitive Systems: 84
Agency Responses to GAO
Questionnaire as of 9-8-88

7%
agencies identifying some sensitive
systems (6)

5%
agencies not responding (4)

88%

agencies identifying all sensitive systems
(74)

CHART 1

CHART 2

Number of Sensitive Systems Reported
by Agencies as of 9-8-88

Air Force (10,000)

5.6%
Other DOD (3,000)

2.7%
Civilian agencies (1,443)

Navy (27,000)

Army (12,000)

50.5%

22.5%

18.7%