MEMORANDUM REPORT 01-IT-M-084
Strong Management Support Needed to Ensure the Broadcasting Board of Governors Complies with the Government Information Security Reform Act
September 2001

In response to the Government Information Security Reform Act (GISRA), Public Law 106-398, the Office of Inspector General (OIG) performed an independent evaluation of the information security program of the Broadcasting Board of Governors (BBG). Specific objectives of our review were to identify the BBG's policies and procedures for securing information on its information systems and to determine whether the BBG is effectively implementing requirements of the Government Information Security Reform Act.

RESULTS IN BRIEF

When OIG began its review in February 2001 BBG did not have a documented, agency-wide information security program as required by GISRA and had not documented security level requirements for its systems. Since then, the BBG has appointed a Chief Information Officer (CIO) and has made some progress toward establishing an information security program. For example, in July 2001, the CIO issued a draft paper outlining a framework for the BBG Information Security Program, including a discussion of roles and responsibilities, training requirements, and the agency's enterprise architecture. OIG is encouraged by these steps to comply with GISRA and recommends that the BBG complete work on developing its information security program by the end of October 2001 and include a discussion of these efforts in its remediation plan, which is due to the Office of Management and Budget on October 31, 2001.

BACKGROUND

The U.S. International Broadcasting Act of 1994 (Public Law 103-236), created the BBG as a self-governing element within the former United States Information Agency, which provided some administrative, technical, and management support to BBG. The Foreign Affairs Reform and Restructuring Act of 1998 (Public Law 105-277) granted the BBG independence from the United States Information Agency on October 1, 1999. BBG is responsible for overseeing all U.S. Government-funded, civilian broadcasting, including the operations of the International Broadcasting Bureau (IBB), which includes the broadcasting entities of Voice of America, Worldnet Television and Film Service, and Office of Cuba Broadcasting. BBG also oversees two grantee organizations—Radio Free Europe/Radio Liberty and Radio Free Asia.

Information security is an important consideration for any organization that depends on information systems and computer networks to carry out its mission or business. Computer-supported government operations, including those at the BBG, are at increasing risk. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, these developments pose enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer networks and systems. Further, the number of people with computer skills is increasing, and intrusion techniques and tools are readily available and relatively easy to use. The rash of cyber attacks launched in February 2000 against major U.S. firms and the global disruption caused by the "ILOVE YOU" virus in May 2000 illustrate the risks associated with this new electronic age.

Faced with growing concerns about information security risks to the Federal Government, the Congress passed and the President signed GISRA into law in late 2000. GISRA provides: (1) a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets; and, (2) a mechanism for improved oversight of Federal agency information security programs. Specifically, GISRA requires each agency to:

- identify, use, and share best security practices;
- develop an agency-wide information security plan;
- incorporate information security principles and practices throughout the life cycles of the agency's information systems; and
- ensure that the information security plan is practiced throughout all life cycles of the agency's information systems.

In addition, GISRA assigns the agency's CIO authority to administer key functions under the statute, including:

- designating a senior agency information security official who shall report to the CIO;
- developing and maintaining an agency-wide information security program;
- ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques; and
- training and overseeing personnel with significant responsibilities for information security.

Finally, in addition to a number of other provisions, GISRA requires that each agency have an annual independent evaluation performed of its information security program and practices. The Inspector General or another independent evaluator performing these evaluations may use any audit, evaluation, or report relating to the effectiveness of the agency's information security program. The agency is required to submit the independent evaluation, along with its own assessment, to the Office of Management and Budget as part of its annual budget request.

PURPOSE, SCOPE, AND METHODOLOGY

Section 3535 of GISRA directs each agency to have conducted an independent evaluation of its information security program and practices. In response to GISRA, the Office of Inspector General conducted this review with the specific objectives of: (1) identifying the BBG's policies and procedures for securing information on its information systems; and (2) determining whether the BBG is in compliance with GISRA with regard to establishing and ensuring the effectiveness of controls over information resources.

To fulfill our review objectives, we met with officials from organizations throughout BBG including the IBB, Voice of America, and Worldnet Television and Film Service. We spoke with officials from the Office of Cuba Broadcasting, but did not conduct any field work at its headquarters in Miami. The Office of Cuba Broadcasting had become aware of GISRA requirements only in June 2001 and requested time to develop and implement compliance measures. Also, OIG did not conduct detailed review work with the BBG's grantee organizations, Radio Free Europe/Radio Liberty, and Radio Free Asia. They are private nonprofit organizations that own and operate their own information technology systems.

In addition to detailed discussions with appropriate BBG management and staff, we developed and used a questionnaire based on the National Institute of Standards and Technology's *Self-Assessment Guide for Information and Technology Systems*. We collected other pertinent supporting information security documentation as appropriate. We did not review technical controls during this evaluation because BBG was still developing its security program. We followed generally accepted government auditing standards and conducted such tests and procedures as were considered necessary to the assignment. We obtained written comments on a draft of this report from BBG and revised the report where appropriate. The BBG's comments are included in Appendix A. Staff from our Information Technology Issue Area performed this evaluation from February 2001 through August 2001. Contributors to this report were Frank Deffer, James Davies, Tim Fitzgerald, Robert Taylor, Anthony Carbone, Sharon Hunter, Chris Watson, and Matthew Worner. Comments or questions about the report can be directed to Mr. Deffer at defferf@state.gov or at (703) 284-2715 or to Mr. Davies at daviesj@state.gov or at (703) 284-2673.

AUDIT FINDINGS

BROADCASTING BOARD OF GOVERNORS SHOWS PROGRESS IN ESTABLISHING AN INFORMATION SECURITY PROGRAM

When OIG began its review in February 2001, the BBG did not have a documented information security program or written policies and procedures covering information security. OIG's independent evaluation revealed that BBG's senior management began actions in early 2001, to respond to GISRA requirements. The BBG is now developing its information systems security program. OIG is supportive of the direction in which the agency is headed at this time and has refrained from making numerous detailed recommendations. OIG encourages BBG senior management and staff to develop the information security program that they believe is best for their agency.

Information Security Controls Required

Upon initiating this evaluation in February 2001, OIG found that BBG had not developed written policies and procedures for establishing commonly used information security controls. OIG found that BBG primarily uses commercial off-the-shelf software and identified 49 systems that it was operating at the time of our evaluation. Using questions taken from the National Institute of Standards and Technology's *Self-Assessment Guide*, OIG held discussions with several system owners and found that they were not using standard information security controls while managing their systems and that system security level determinations had not been documented. Furthermore, other key items that would support a stronger risk management approach to information security as called for under GISRA were missing. They include:

- risk assessments;
- contingency plans;
- vulnerability testing;
- an information security training program; and
- procedures for detecting, reporting, and responding to security incidents.

BBG Takes Steps to Develop an Agency-wide Systems Security Program and Plans

Since February 2001, the agency has taken a number of steps to develop an information security program to meet GISRA requirements. Specifically, the BBG designated IBB's associate director for management as the CIO. The CIO is responsible for establishing agency information management policy and for administering the agency's information security program. In July 2001, the CIO issued a draft outline of a framework for the BBG's Information Security Program, including a description of:

- roles and responsibilities of key officials, such as the CIO, program officials, office directors, the Broadcast Technology Steering Committee, and the user;
- training requirements to ensure that employees understand their security obligations; and

- BBG’s enterprise architecture, including an overview of the agency’s global computing environment.

In addition, five BBG program offices—Computing Services, Engineering and Technical Services, Voice of America Broadcast Operations, the Office of Cuba Broadcasting, and the Office of Internet Development—are developing security plans to protect BBG’s 18 mission-critical and 31 nonmission-critical systems that were identified during our evaluation. The development of these security plans, according to BBG officials, is geared toward meeting GISRA requirements. Overall, these efforts suggest that BBG is making steady progress toward establishing an effective information security program throughout the agency.

Recommendation 1: We recommend that the Broadcasting Board of Governors direct the Chief Information Officer to complete the development of the agency’s information security program by the end of October 2001 and that noted issues in this report be addressed not later than October 31, 2001, as part of the Board’s remediation process and plan under the Government Information Security Reform Act.

BBG Response

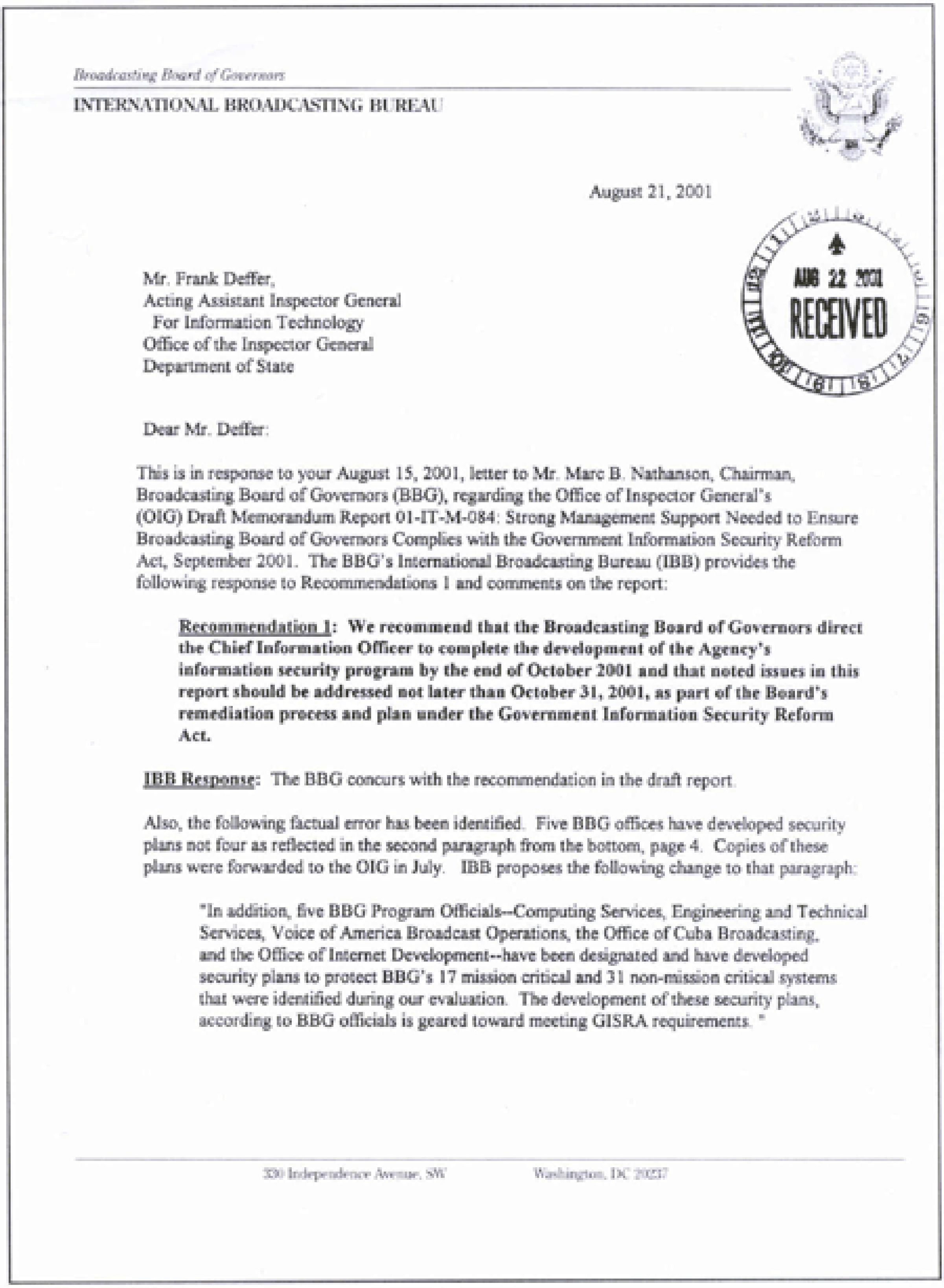
In commenting on a draft of this report (see Appendix A), the BBG concurred with this recommendation. Also, the BBG noted one factual error in the draft report.

OIG Comment

The Inspector General accepts this response and considers this recommendation resolved. The BBG should provide OIG with copies of the BBG’s remediation plan when it is submitted to the Office of Management and Budget on October 31, 2001, for consideration in closing this recommendation.

OIG has corrected the factual error noted by the BBG in its response to the draft report.

APPENDIX A



Broadcasting Board of Governors

INTERNATIONAL BROADCASTING BUREAU

August 21, 2001

Mr. Frank Deffer,
Acting Assistant Inspector General
For Information Technology
Office of the Inspector General
Department of State

Dear Mr. Deffer:

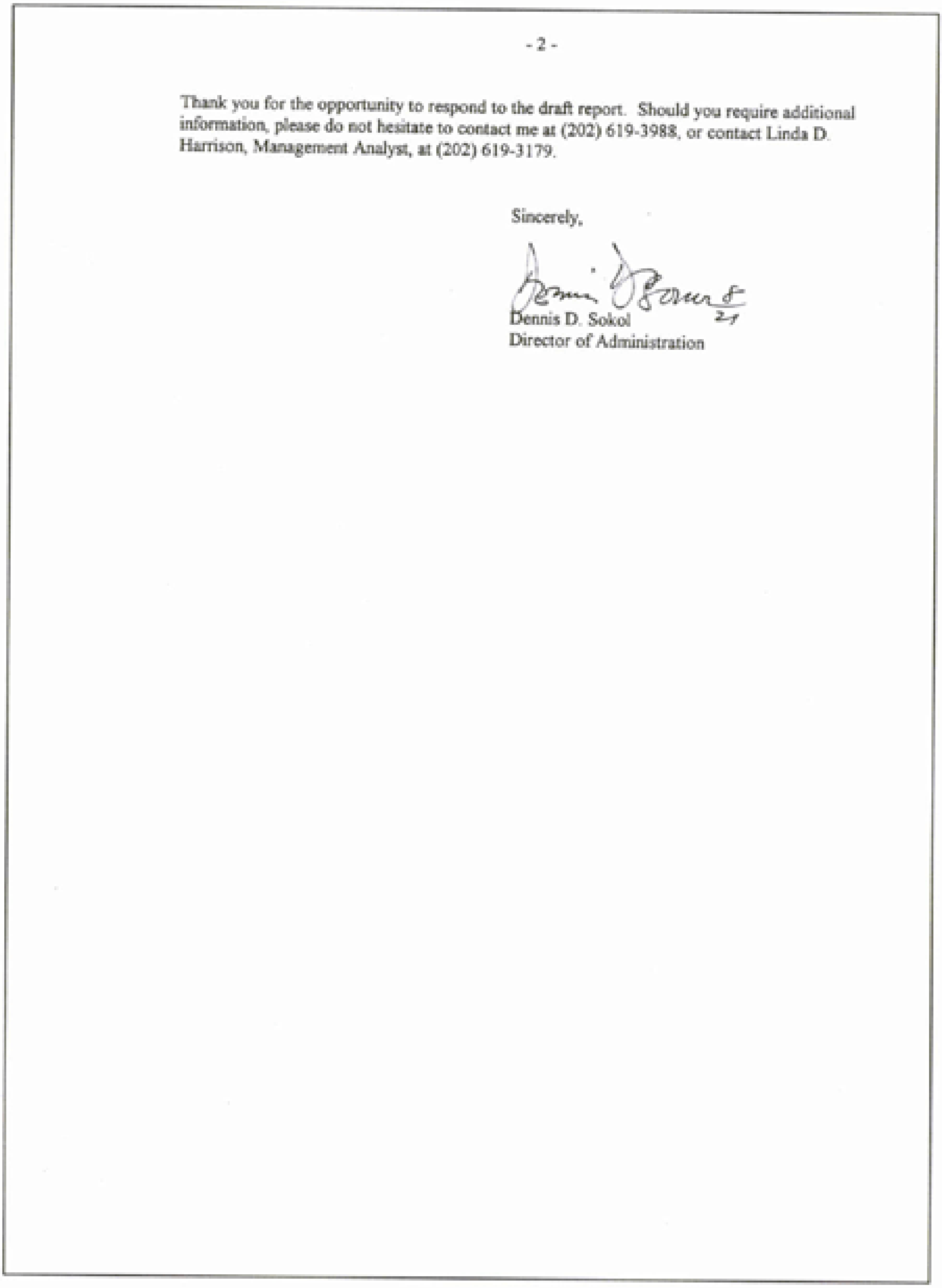
This is in response to your August 15, 2001, letter to Mr. Marc B. Nathanson, Chairman, Broadcasting Board of Governors (BBG), regarding the Office of Inspector General's (OIG) Draft Memorandum Report 01-IT-M-084: Strong Management Support Needed to Ensure Broadcasting Board of Governors Complies with the Government Information Security Reform Act, September 2001. The BBG's International Broadcasting Bureau (IBB) provides the following response to Recommendations 1 and comments on the report:

> **Recommendation 1: We recommend that the Broadcasting Board of Governors direct the Chief Information Officer to complete the development of the Agency's information security program by the end of October 2001 and that noted issues in this report should be addressed not later than October 31, 2001, as part of the Board's remediation process and plan under the Government Information Security Reform Act.**

IBB Response: The BBG concurs with the recommendation in the draft report.

Also, the following factual error has been identified. Five BBG offices have developed security plans not four as reflected in the second paragraph from the bottom, page 4. Copies of these plans were forwarded to the OIG in July. IBB proposes the following change to that paragraph:

> "In addition, five BBG Program Officials--Computing Services, Engineering and Technical Services, Voice of America Broadcast Operations, the Office of Cuba Broadcasting, and the Office of Internet Development--have been designated and have developed security plans to protect BBG's 17 mission critical and 31 non-mission critical systems that were identified during our evaluation. The development of these security plans, according to BBG officials is geared toward meeting GISRA requirements. "



Thank you for the opportunity to respond to the draft report. Should you require additional information, please do not hesitate to contact me at (202) 619-3988, or contact Linda D. Harrison, Management Analyst, at (202) 619-3179.

Sincerely,

8/21

Dennis D. Sokol
Director of Administration