AR 08-004

Office of Inspector General

Independent Evaluation Report

Review of Federal Trade Commission Implementation of the Federal Information Security Management Act For Fiscal Year 2008

September 30, 2008

NON PUBLIC REPORT

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Inspector General

September 30, 2008

Chairman Kovacic:

The Office of Inspector General (OIG) for the Federal Trade Commission engaged Allied Technology, Inc. to independently evaluate its information security for compliance with requirements contained in the Federal Information Security Management Act (FISMA) of 2002. This report provides the results of that evaluation.

The objectives were to evaluate the adequacy of the FTC's information security program and its procedures for identifying and protecting Personally Identifiable Information (PII) and other Privacy Act concerns. This information is provided to senior management and others to enable them to determine the effectiveness of overall security programs, to ensure the confidentiality and integrity of data entrusted to the FTC, and to develop strategies/best practices for cost effectively improving information security.

The OIG reviewed the FTC's security policies, procedures, and practices and conducted an assessment of security controls in the following areas:

REDACTED

This evaluation was conducted from June through September 2008 and followed standards and requirements for federal government agencies such as those provided through FISMA, National Institute of Standards and Technology and the Office of Management and Budget memorandums.

The FTC security environment is strong and robust and continues to evolve to expand its coverage. REDACTED REDACTED

b)(2) REDACTED The Information and Technology Management Office (ITM) took actions that addressed REDACTED recommendations at Headquarters and REDACTED recommendations at the REDACTED The

OIG analysis of the current FTC security/privacy control environment identified 12 findings at [REDACTED] (b)(2)
Generally, the recommendations addressed two areas. [REDACTED]
[REDACTED] The major effort for ITM next year will be its focus on [REDACTED]

OIG commends ITM on its efforts to assure a secure IT environment at the FTC and to thank ITM management for the cooperation and assistance it provided to the OIG during our review.

Respectfully submitted,

John M. Seeba
Inspector General

AR 08-004

Office of Inspector General

Independent Evaluation Report

Review of Federal Trade Commission Implementation of the Federal Information Security Management Act For Fiscal Year 2008

September 30, 2008

NON PUBLIC REPORT

Federal Trade Commission
Evaluation of the Federal Information Security Management Act of 2002

Submitted to:

The Federal Trade Commission
Office of the Inspector General
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
ATTN: John Seeba
Inspector General

Submitted by:

Allied Technology Group, Inc.
1803 Research Boulevard
Rockville, Maryland 20850

Contract Number: GS-35F-0079J
Task Order Number: FTC-07-G-7114

TABLE OF CONTENTS

Table of Figures

EXECUTIVE SUMMARY

Results in Brief

The Federal Trade Commission (FTC) is an independent agency responsible for the administration of a variety of statutes that are designed to promote competition and to protect the public from unfair and deceptive acts and practices in the advertising and marketing of goods and services.

These responsibilities often result in the accumulation of vast quantities of records, some of which contain sensitive information. Automated information systems have been developed or acquired to assist FTC staff in conducting their law enforcement and management efforts. This includes collection of information from commercial organizations and the general public. Information in these systems and systems functionality is made available to FTC employees based on their organizational role. Access to selected information is available to the public on a read-only basis via the Internet. The agency also relies on automated files and records to pay its employees and vendors, process personnel transactions, and perform other "housekeeping" functions.

The Information and Technology Management (ITM) Office is responsible for the technological infrastructure and the office systems that provide the FTC with the tools and the information needed to conduct and manage its consumer protection and competition missions. Responsibility for establishing and maintaining the FTC information assurance/security program is assigned to the Chief Information Security Officer who reports to the Chief Information Officer. Responsibility for the FTC Privacy Program is assigned to the Chief Privacy Officer who reports to the FTC Chief of Staff.

The Federal Information Security Management Act of 2002 (FISMA) provides a comprehensive framework for ensuring the effectiveness of technical, administrative, and physical security controls over information resources that support Federal operations and assets. FISMA requires an annual assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. The assessments are meant to provide agency senior management and others with the needed information to determine the effectiveness of overall security programs, ensure the confidentiality and integrity of data entrusted to the FTC, and to develop strategies/best practices for cost effectively improving information security.

A critical component of the FISMA information assurance program monitoring requirements is an independent assessment of program effectiveness by the Inspector General (IG) of the respective federal agency. This assessment is intended to identify weaknesses in agency programs, provide recommendations for corrective actions, and monitor agency success in maintaining the security of agency information assets (hardware, software, data, and system availability). In its FY 2008 FISMA reporting guidance, OMB expanded the scope of the annual FISMA assessment to include evaluation of agency policies and procedures for collecting, storing, and protecting privacy information.

The Office of Inspector General (OIG) reviewed FTC security policies, procedures, and practices and conducted detailed assessments of FTC security and privacy controls in the following areas:

(b)(2) REDACTED

This report provides the results of the independent evaluation of the FTC information security environment by the Office of the Inspector General (OIG). The results are current as of September 30, 2008 and provide the evaluation of the adequacy of the FTC's information security program and practices for Fiscal Year 2008 (FY 2008).

Findings in Brief

The FTC security environment is strong and robust and continues to evolve to expand its coverage and to address changing threats and requirements. FTC management recognizes that continued vigilance, and resource investment is required to protect the data entrusted to its care and secure the availability and integrity of the information technology (IT) systems that are critical to the agency's ability to successfully complete its missions.

The FTC Office of Information Technology Management (ITM) is continuing its effort to update its security policies and procedures. This effort is integrated with the FTC Privacy Program. Integration of the FTC Information and Privacy programs will result in stronger protection than independent program efforts.

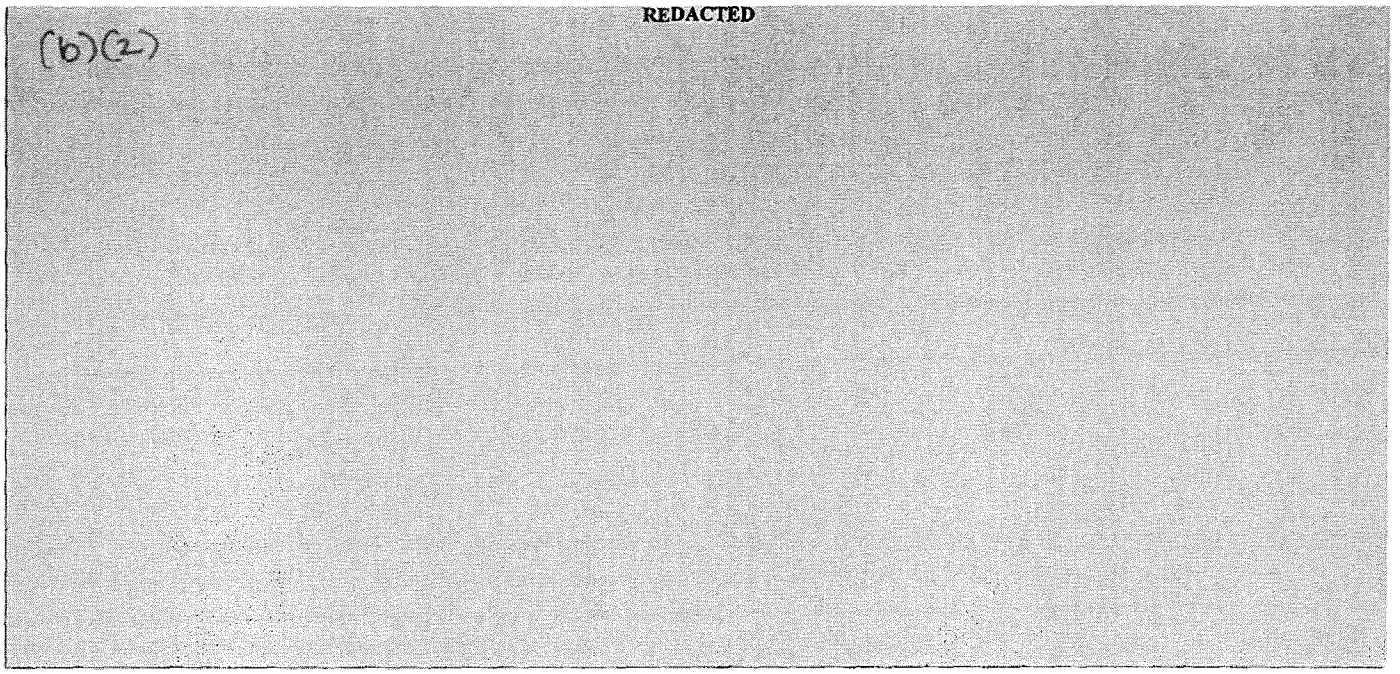
The OIG analysis of the current FTC security/privacy control environment identified REDACTED findings. The findings related to REDACTED

(b)(2) REDACTED REDACTED REDACTED

The following table lists the findings and recommendations developed through this FY 2008 FISMA evaluation.

REDACTED

(b)(2)



1.0 BACKGROUND

The Federal Trade Commission (FTC) is an independent agency responsible for the administration of a variety of statutes that are designed to promote competition and to protect the public from unfair and deceptive acts and practices in the advertising and marketing of goods and services.

These responsibilities often result in the accumulation of vast quantities of records, some of which contain sensitive information. Automated information systems have been developed to assist FTC staff in conducting their law enforcement and management efforts. [REDACTED] Access to selected information is available to the public on a read-only basis via the Internet. The agency also relies on automated files and records to pay its employees and vendors, process personnel transactions, and perform other "housekeeping" functions formally performed manually.

(b)(2)

In the past few years, the FTC has expanded its use of the Internet to support public-focused missions such as establishment of the "Do Not Call Registry" and collecting complaints regarding companies, business practices, identity theft, and episodes of violence in the media. The implementation of these mission-support systems increased the need for the FTC to establish and maintain an information security environment that both protects information assets (hardware, software, data) without being so restrictive that it limits intended use by the general public.

The Information and Technology Management (ITM) Office, in the Office of the Executive Director, is responsible for the technological infrastructure and the office systems that provide the FTC with the tools and the information needed to conduct and manage its consumer protection and competition missions.

The Federal Information Security Management Act of 2002 (FISMA) provides a comprehensive framework for ensuring the effectiveness of technical, administrative, and physical security controls over information resources that support Federal operations and assets. FISMA requires an annual assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. The assessments are meant to provide agency senior management and others with the information needed to determine the effectiveness of overall security programs, ensure the confidentiality and integrity of data entrusted to the FTC, and to develop strategies/best practices for cost effectively improving information security.

The Office of Management and Budget (OMB) through Circular A-130, *Management of Federal Information Resources, Appendix III,* provides guidance to federal agencies regarding the implementation of FISMA requirements. OMB Circular A-130 emphasizes that, under FISMA, Agencies are required to implement, maintain, and enhance an automated information assurance program, including the preparation of policies,

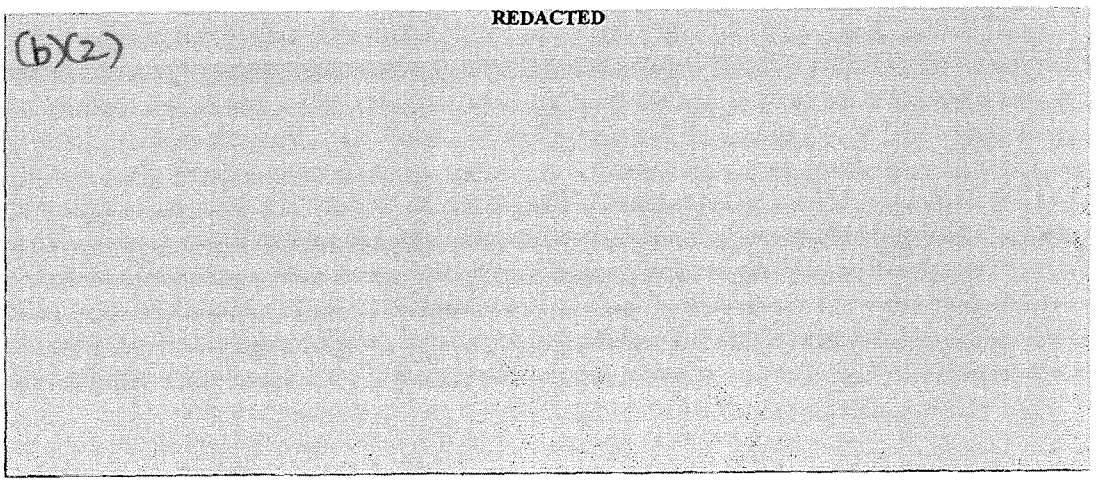
standards, and procedures for providing information security and monitoring program effectiveness. Establishing and maintaining an effective information security program is an important managerial responsibility. The OMB also provides guidance regarding the scope and information to be reported through the annual FISMA assessments. In 2008, OMB guidance expanded the scope of the annual FISMA assessments to address concerns regarding the protection afforded information related to individuals (i.e., privacy data).

A critical component of the FISMA information assurance program monitoring requirements is an independent assessment of program effectiveness by the Inspector General (IG) of the respective federal agency. This assessment is intended to identify weaknesses in agency programs, provide recommendations for corrective actions, and monitor agency success in maintaining the security of agency information assets (hardware, software, data, and system availability). An independent assessment is especially critical because threats to federal information assets are continuously changing as technology evolves and the number and complexity of attacks on federal systems is increasing. The independent assessment provides an opportunity to examine security controls and security planning and ensure that the controls are addressing the changed security environment and the increased focus on protecting information related to individual privacy.

This report provides the results of the independent evaluation of the FTC information security environment by the Office of the Inspector General (OIG). The results are current as of September 30, 2008 and provide the evaluation of the adequacy of the FTC's information security program and practices for fiscal year 2008 (FY 2008).

2.0 SCOPE

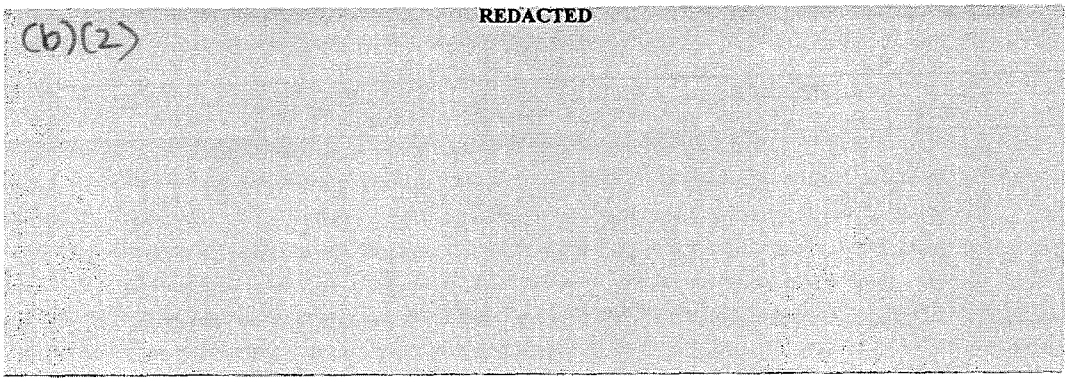
To accomplish this FISMA evaluation, the OIG reviewed FTC security policies, procedures, and practices and conducted an assessment of FTC security controls in the following areas:



This assessment focused on the FTC procedures and practices used to maintain and evolve its information security controls. This approach provides an assessment of the capability to maintain effective security as well as a "snapshot" of the status of the FTC security environment.

3.0 OBJECTIVE(S)

The objectives of this evaluation are to provide—



All analyses were performed in accordance with the following guidance:

1. Office of Management and Budget (OMB) Memorandum M-05-15, *Reporting Instructions for the Federal Information Security Management Act*, June 13, 2005;

2. OMB M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 27, 2007;

3. OMB M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*, January 18, 2008;

4. OMB M-08-21, FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 14, 2008;

5. FTC policies and procedures

6. *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems*, December 1998;

7. *NIST SP 800-30, Risk Management Guide for Information Technology Systems*, July 2004;

8. *NIST SP 800-34, Contingency Planning Guide for Information Technology Systems*, June 2002;

9. *NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004;

10. *NIST SP 800-53, Recommended Security Controls for Federal Information Systems, Rev. 1*, Dec 2006;

11. *NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems*, June 2008;

12. *Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems*, February 2004;

13. Small Agency Council Memorandum SACCIO-05-1;

14. Quality Standards for Inspection issued by the President's Council on Integrity and Efficiency;

15. GAO, *Federal Information System Controls Audit Manual, Volume I: Financial Statement Audits*, January 1999;

16. FTC/OIG guidance;

17. OMB Memorandum M-03-22, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002*; and

18. OMB Guidance M-04-15, *Guidance for Development of Homeland Security Directive (HSPD) – 7 Critical Infrastructure Protection Plans to Protect Federal Infrastructure and Key Resources.*

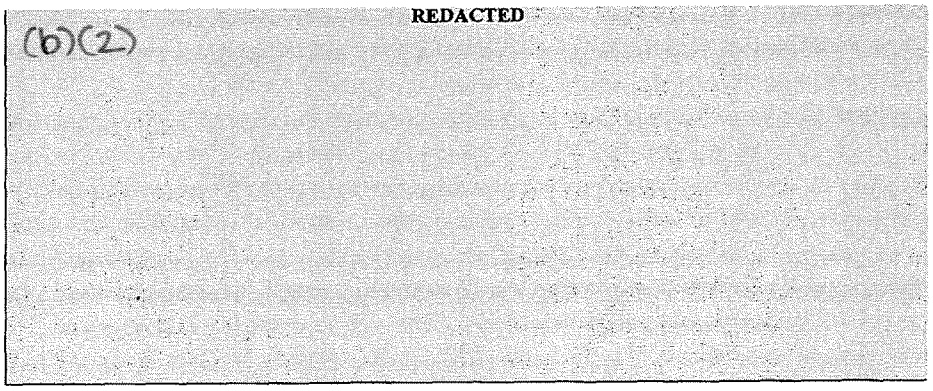
This evaluation was conducted from June, 2008 through September, 2008.

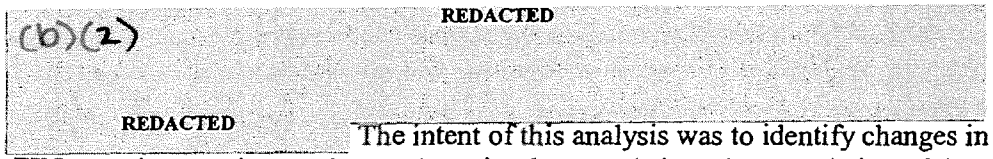
4.0 Methodology

This evaluation constitutes the annual evaluation required by the OMB and conforms to the requirements and guidance provided by the National Institute of Standards and Technology (NIST) through Federal Information Processing Standards (e.g., FIPS 199 and 200) and series 800 Special Publications (e.g., SP 800-53, 800-53A).

The following methodology was used to conduct the overall security control evaluation.

- Planned the Evaluation – Developed a project plan that delineated the evaluation approach and areas of concern for the FY 2008 assessment;
- Collected available published data – Documents containing data relevant to the evaluation was collected. This included:



- 

The intent of this analysis was to identify changes in FTC security practices and procedures implemented since the completion of the FY 2007 FISMA assessment;
- 

- Interviewed FTC staff – Conducted interviews of FTC staff to validate documentation, discuss identified concerns, and evaluate the level of senior management involvement with security planning and performance. The FTC staff interviewed included the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), Chief Privacy Officer (CPO) and members of the ITM;

- Developed preliminary findings – Evaluated the data collected and discussed findings and recommendations with FTC staff. This ensured the accuracy of findings and viability of recommendations; and

- Prepared FY 2008 FISMA report – The information collected and the associated findings and recommendations were used to prepare this FY 2008 FTC FISMA report.

5.0 GENERAL OVERVIEW

REDACTED

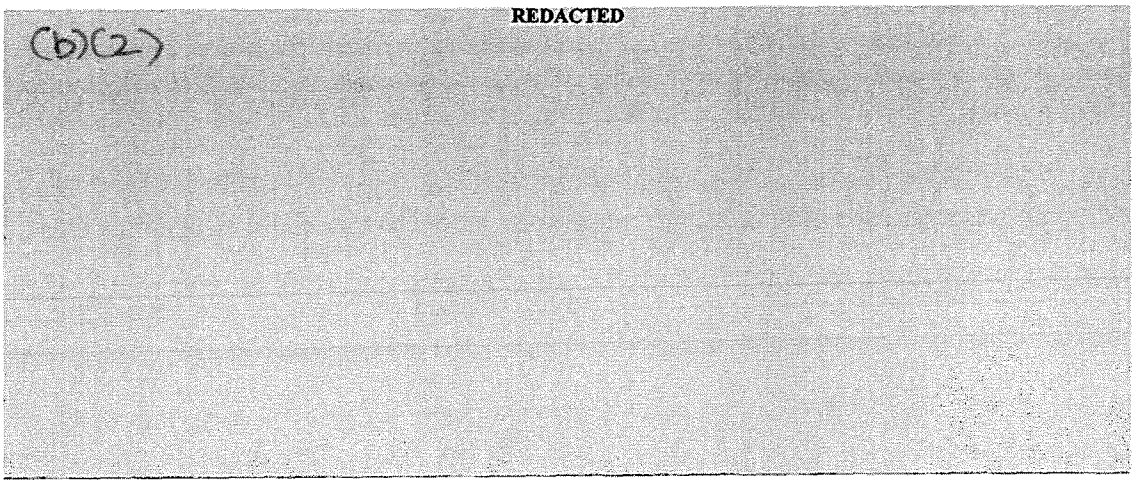
(b)(2)

(b)(2) In general, the FTC security program is strong and robust. REDACTED REDACTED. The level of awareness of security issues and the concern for protecting FTC assets is high. There are procedures in place to monitor program performance and to quickly respond to identified vulnerabilities and opportunities for program enhancement. For example, during the course of this

(b)(2) evaluation, REDACTED REDACTED

The FTC information security and privacy programs need to continue to evolve and enhance their control environments. FISMA expanded the security coverage from a focus on computer system security to a focus on information security. The expansion of the scope of the FISMA evaluations was further expanded this year with the addition of areas of concern specific to protection of Personally Identifiable Information (PII). This continuing expansion REDACTED REDACTED

(b)(2)



The FTC is perceived as a focus of security information by the general public. The public looks to the FTC to provide information as to how to protect its information assets from threats such as identity theft and to protect their privacy through activities such as the *Do Not Call Registry*. This perception is crucial to the FTC's ability to obtain the information and public support it needs to effectively complete its missions. Public confidence in the FTC's ability to protect information requires a continuing focus on security and privacy. The FTC management's continuing emphasis on providing a secure computing environment shows that it recognizes the importance of security and privacy controls to the successful completion of its missions.

6.0 Findings and Recommendations

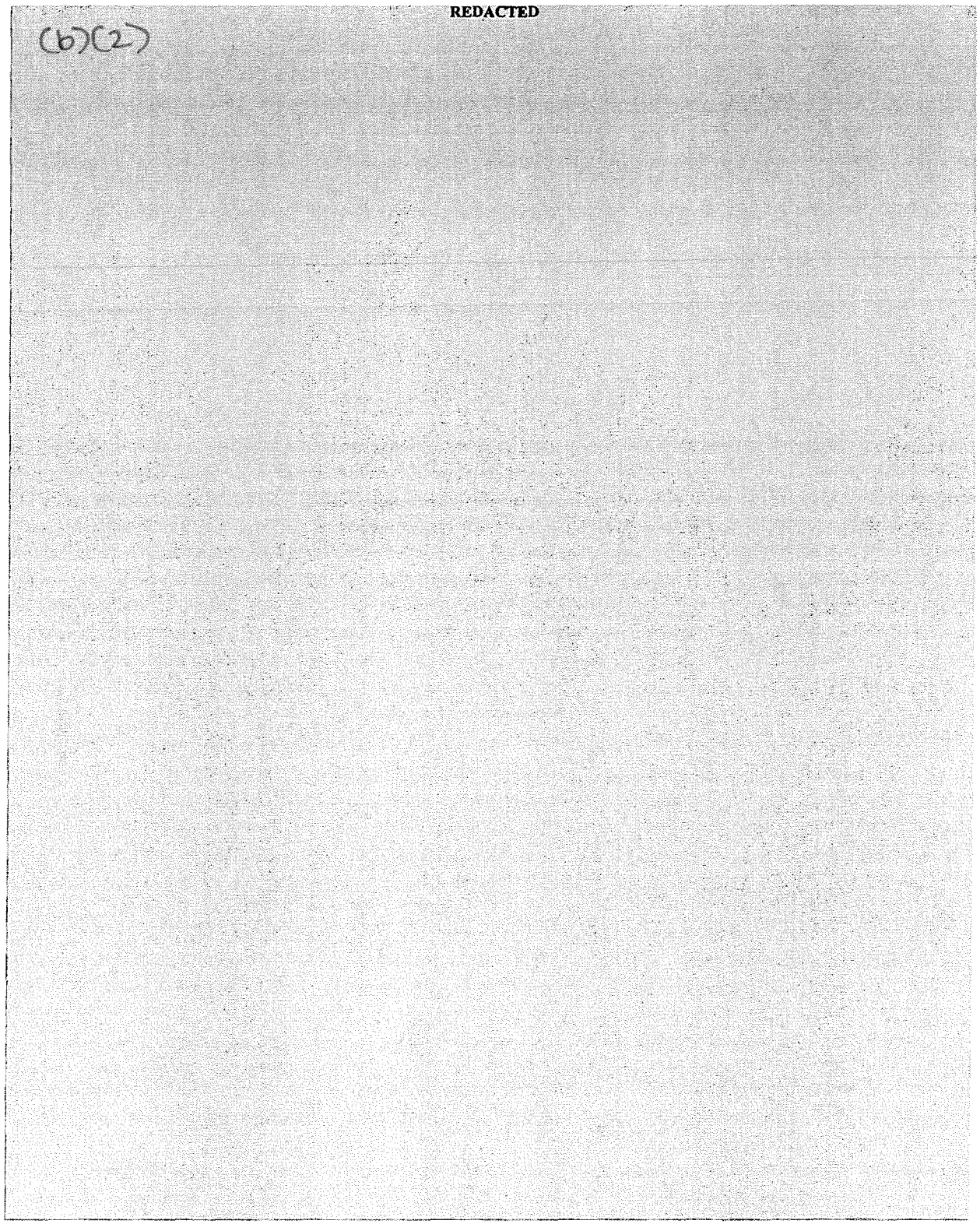
This section presents findings and recommendations developed through the FY 2008 FISMA evaluation.

REDACTED

(b)(2)

REDACTED

(b)(2)



REDACTED

(b)(2)

REDACTED

(b)(2)

Agency Response: REDACTED (b)(2) REDACTED

REDACTED

(b)(2)

Agency Response: REDACTED (b)(2) REDACTED

REDACTED

(b)(2)

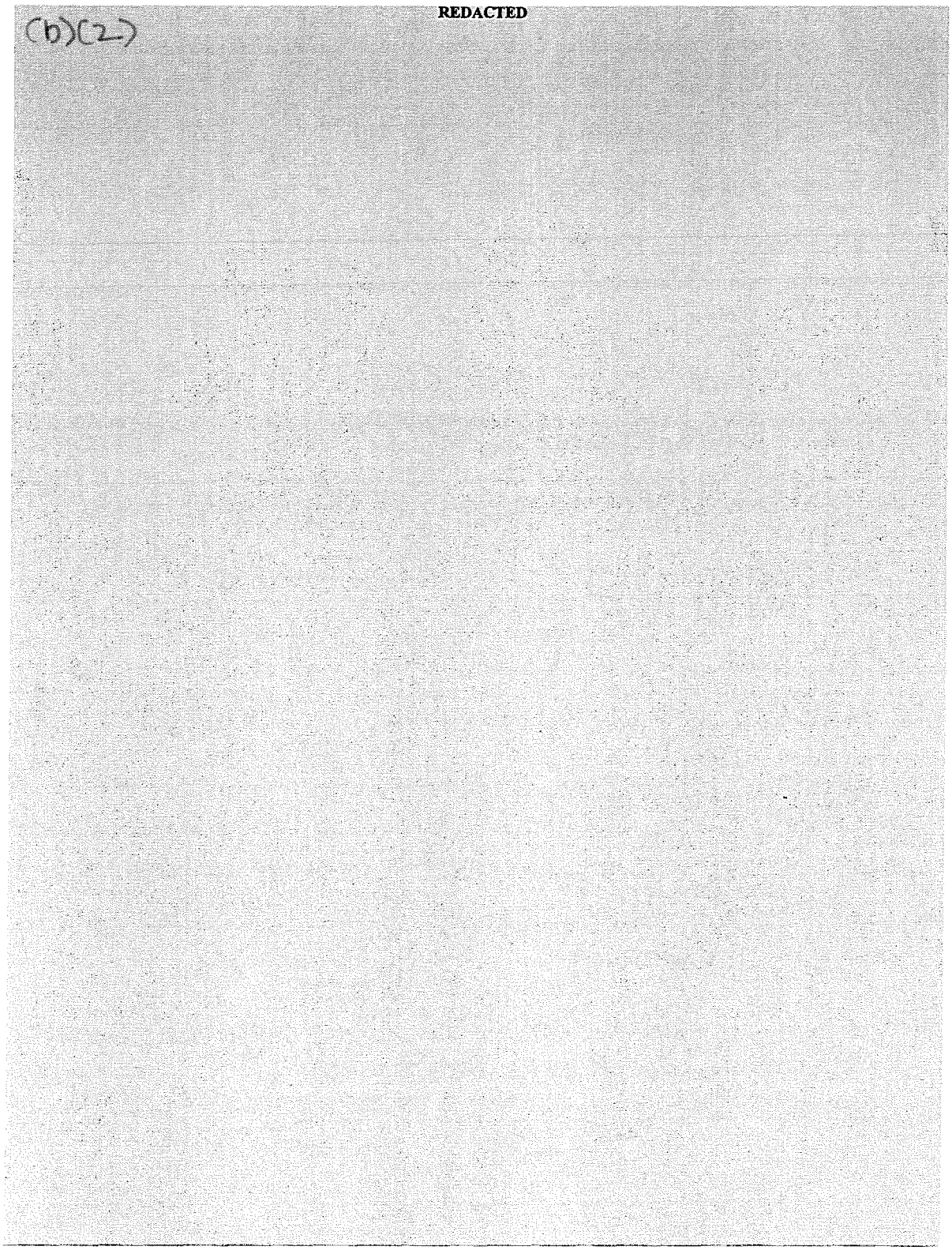
(b)(2) REDACTED

Agency Response: (b)(2) REDACTED REDACTED

(b)(2) REDACTED

REDACTED

(b)(2)



(b)(2) REDACTED

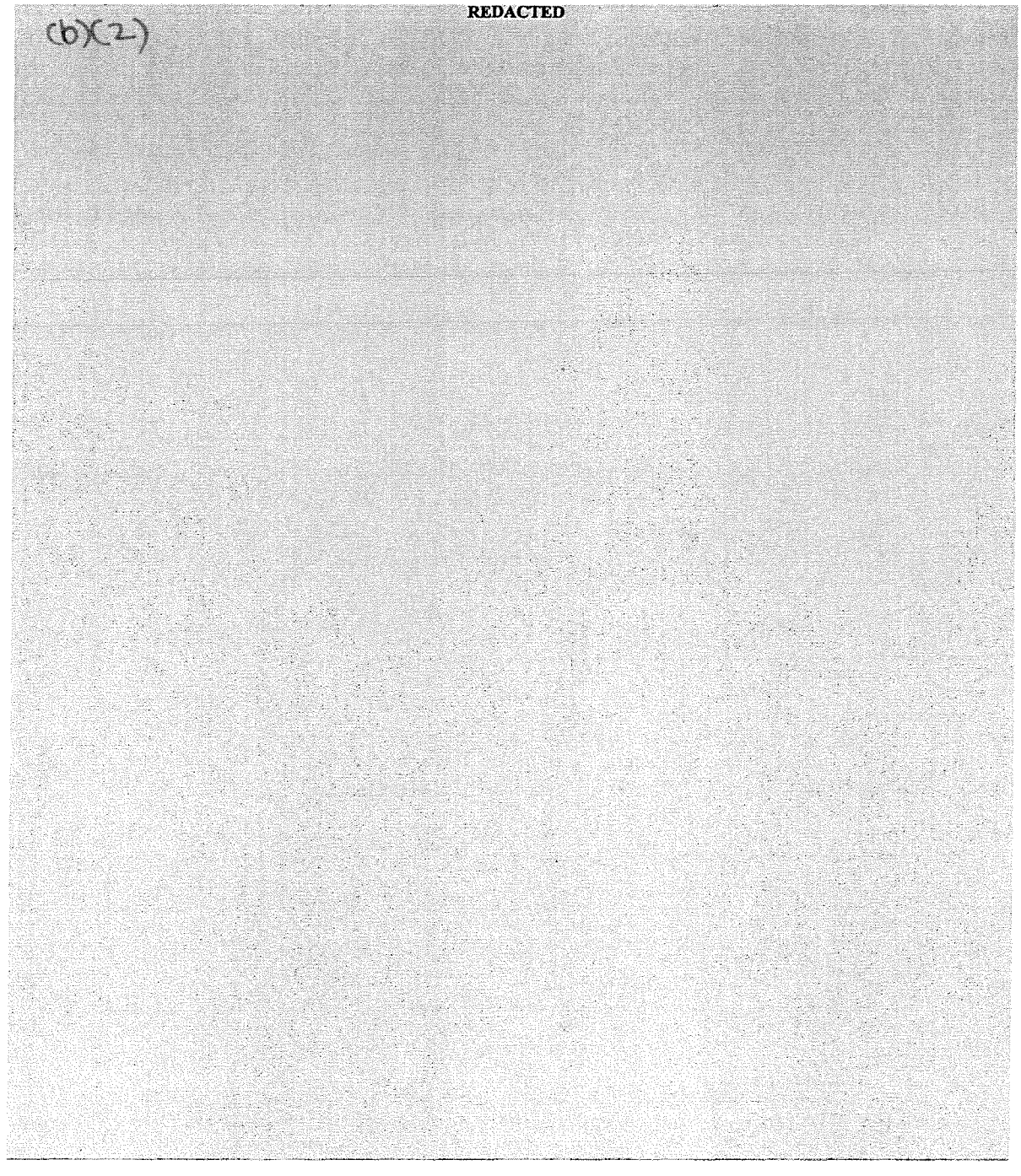
Recommendation: None.

Agency Response: No response required.

(b)(2) REDACTED

Agency Response: (b)(2) REDACTED REDACTED

(b)(2) REDACTED


(b)(2)
REDACTED

REDACTED

(b)(2)

Agency Response: REDACTED (b)(2)

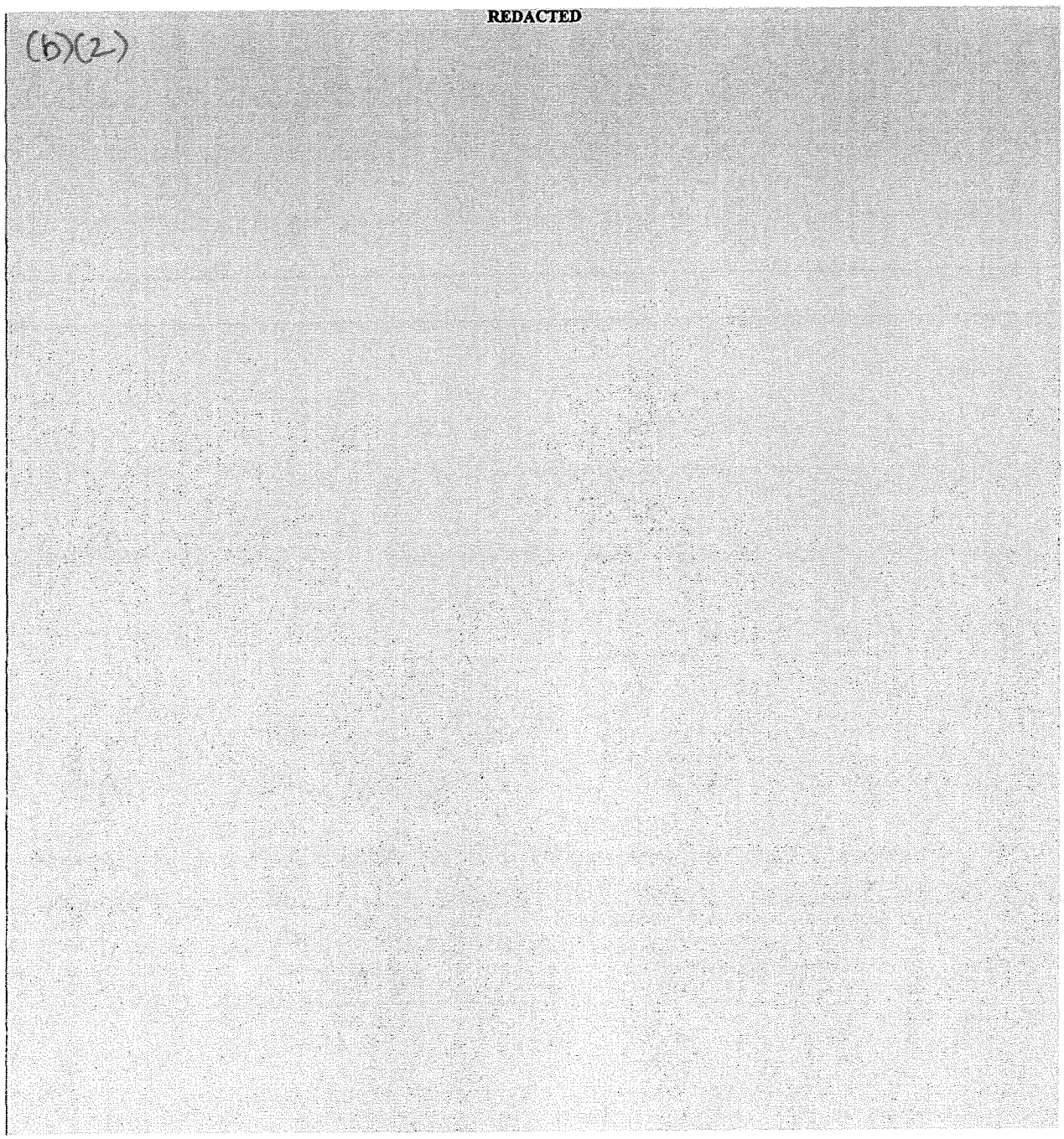
REDACTED

(b)(2)

Agency Response: REDACTED (b)(2)

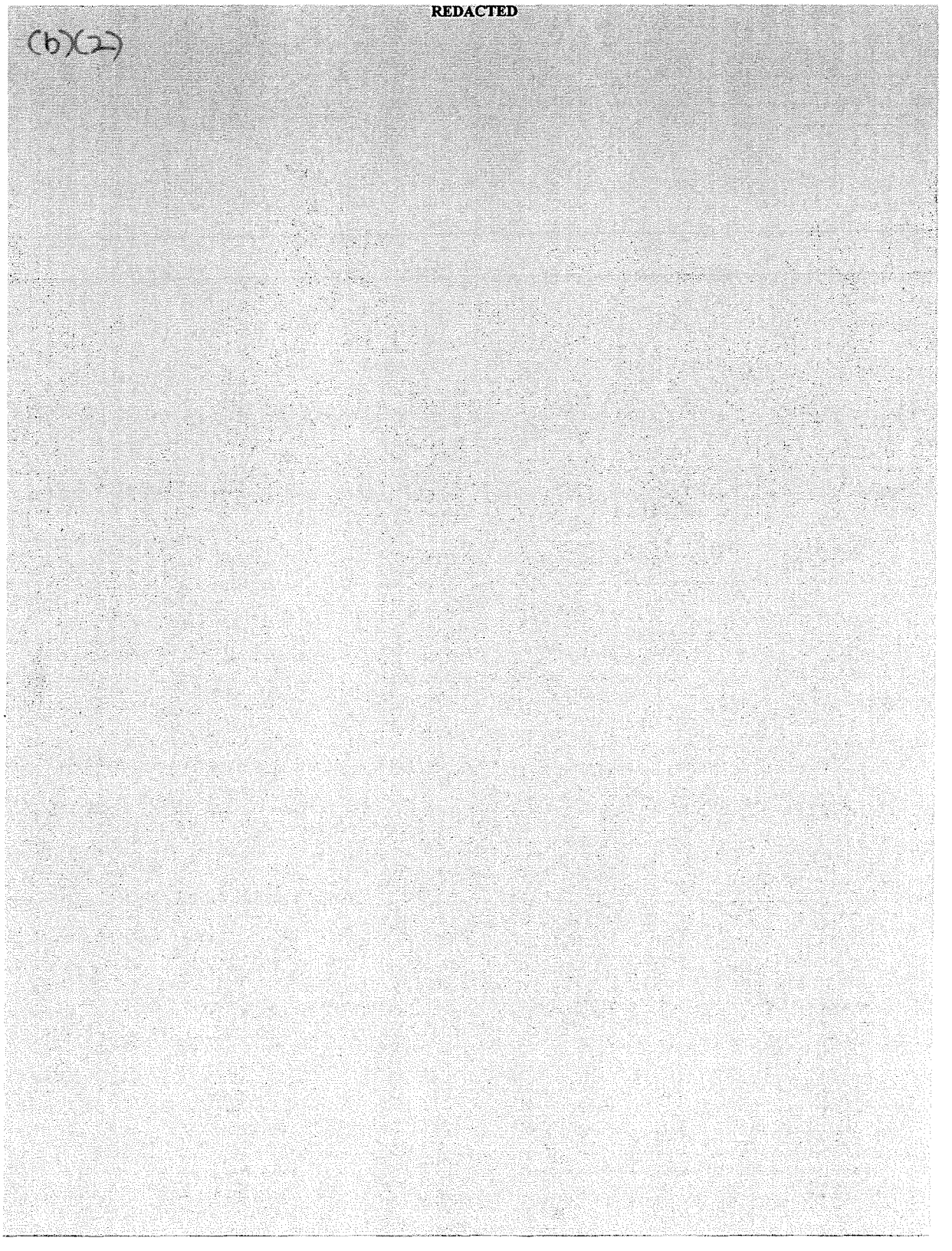
REDACTED

(b)(2)


REDACTED
(b)(2)

REDACTED

(b)(2)



(b)(2) REDACTED

Agency Response: (b)(2) REDACTED REDACTED

(b)(2) REDACTED

Agency Response: (b)(2) REDACTED

(b)(2) REDACTED

REDACTED

(b)(2)

Agency Response:

REDACTED

REDACTED

(b)(2)

REDACTED

(b)(2)

(b)(2)

REDACTED

Agency Response:

REDACTED

(b)(2)

REDACTED

(b)(2)

REDACTED

REDACTED

(b)(2)

Agency Response:

REDACTED

REDACTED

(b)(2)

REDACTED

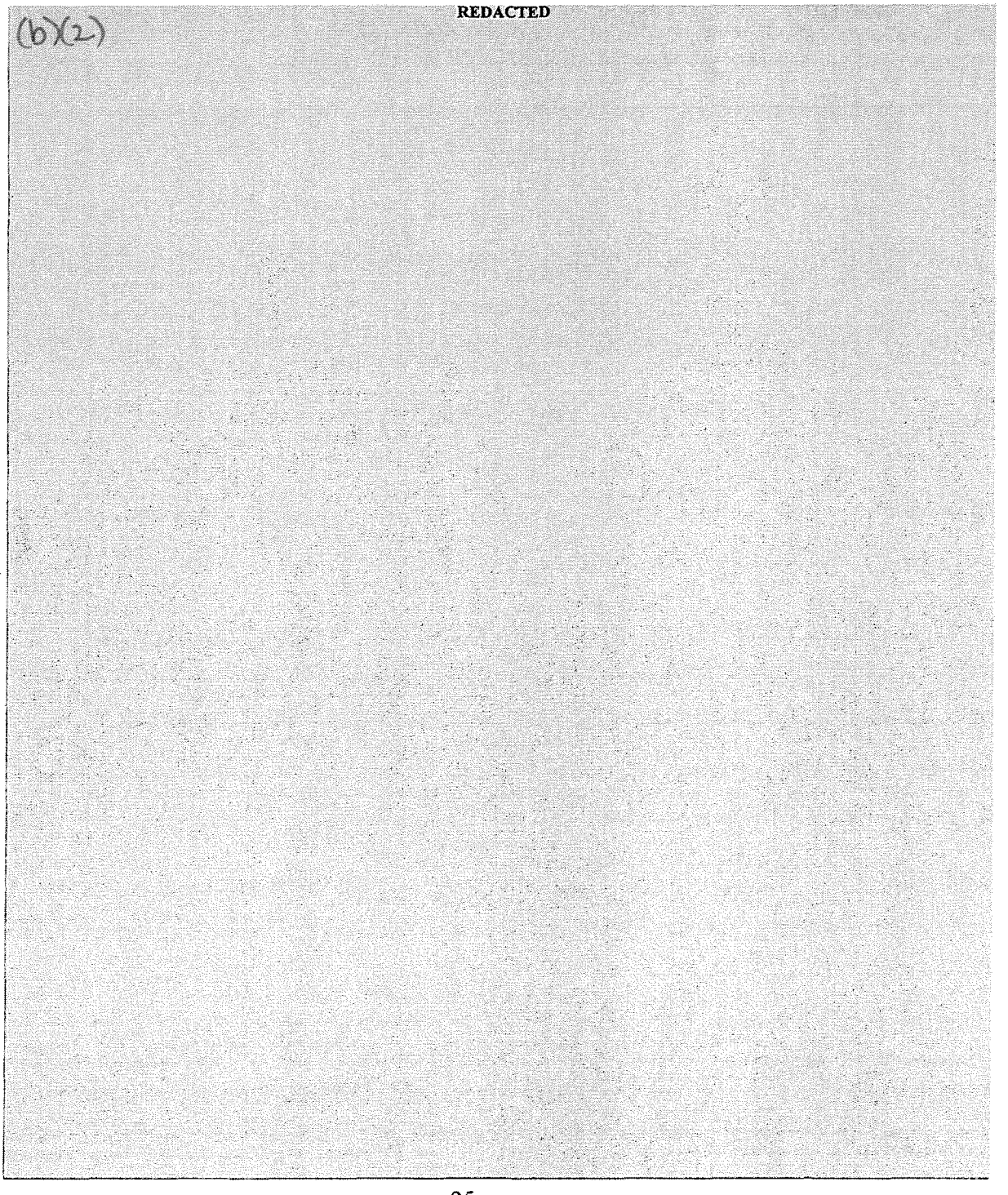
(b)(2)

[3] FAR case 2007-004

7.0 STATUS OF FISCAL YEAR 2007 RECOMMENDATIONS

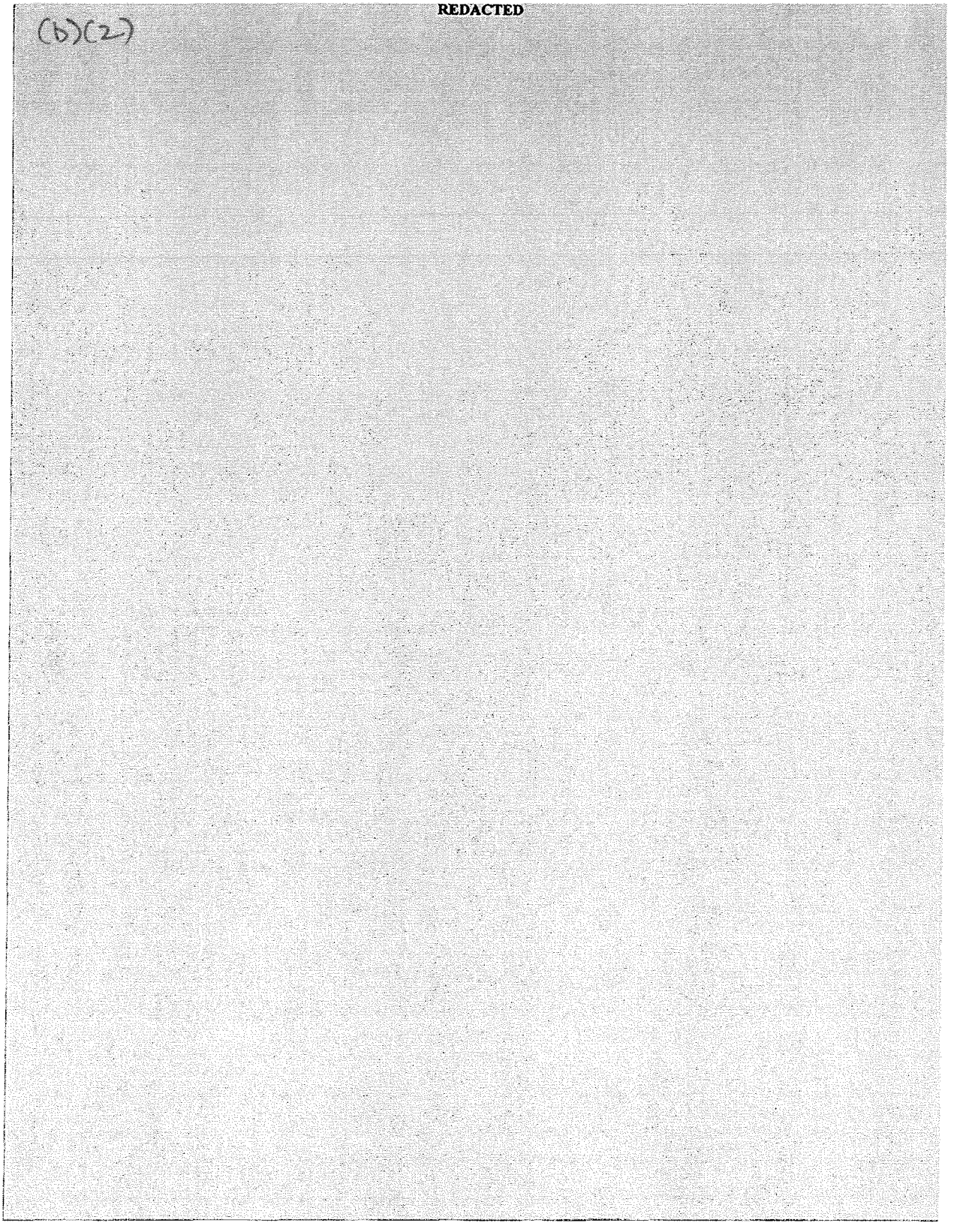
In its FY 2007 FISMA report, the OIG identified REDACTED FTC information security environment. (b)(2) REDACTED

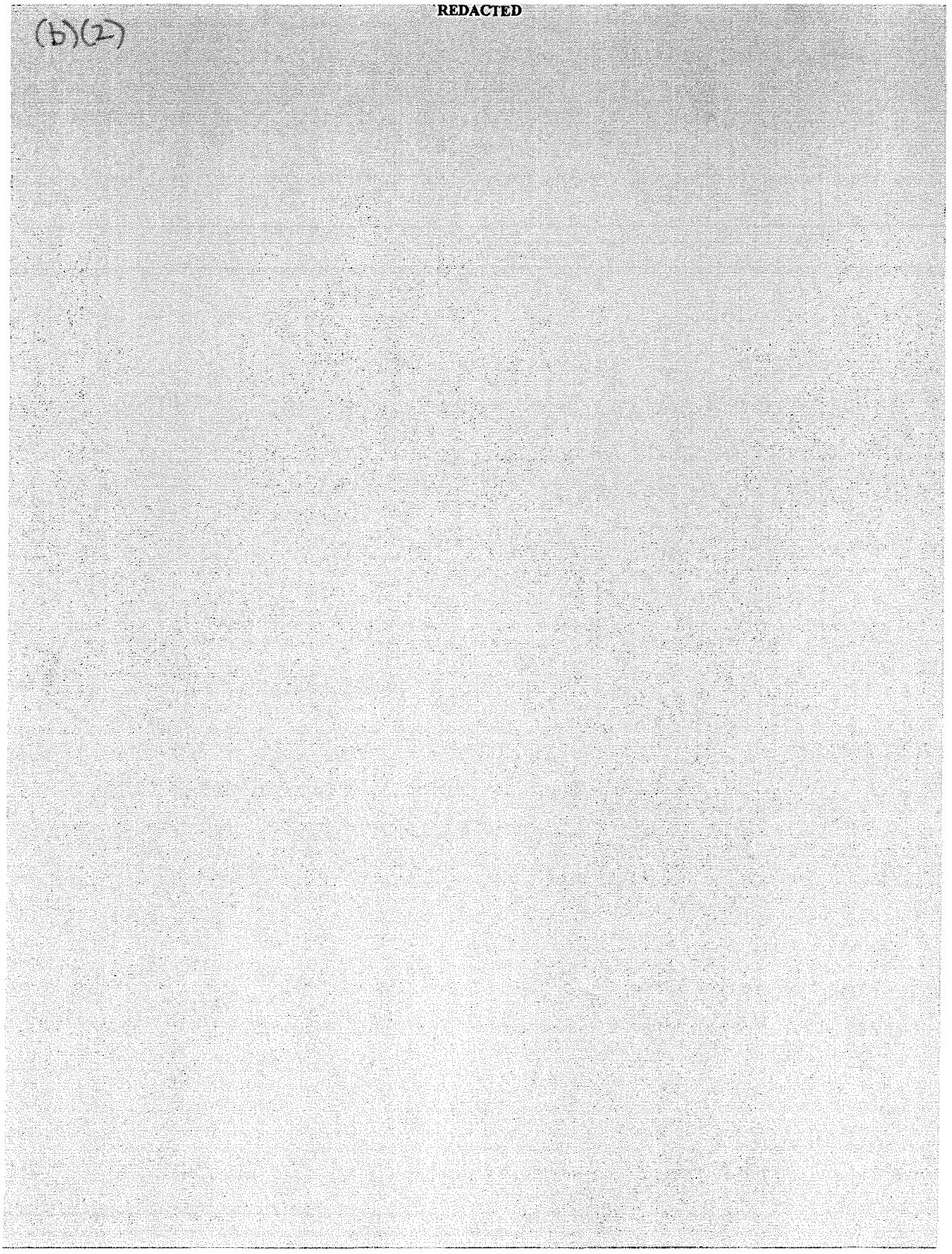
(b)(2)

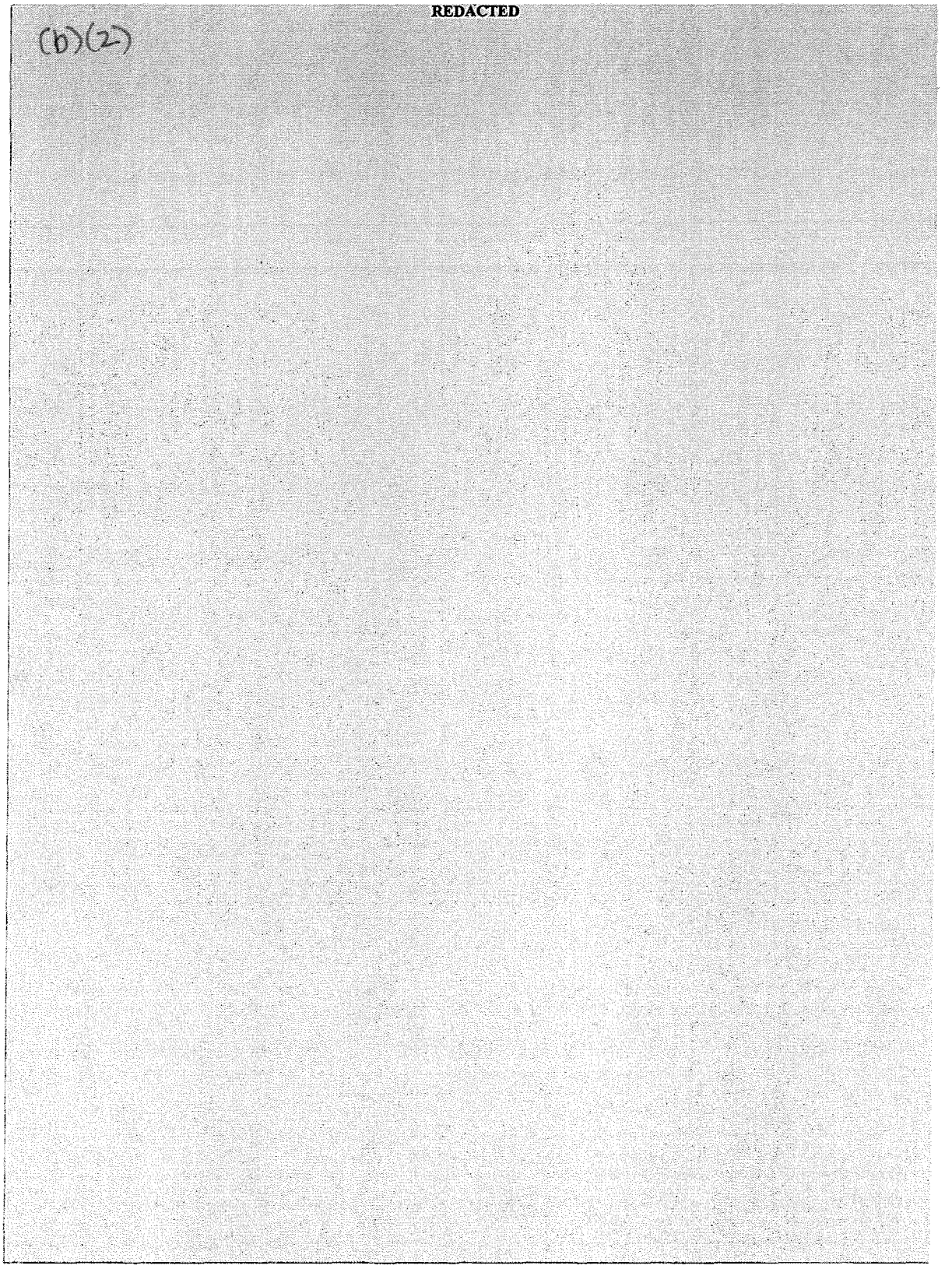


(b)(2)

REDACTED

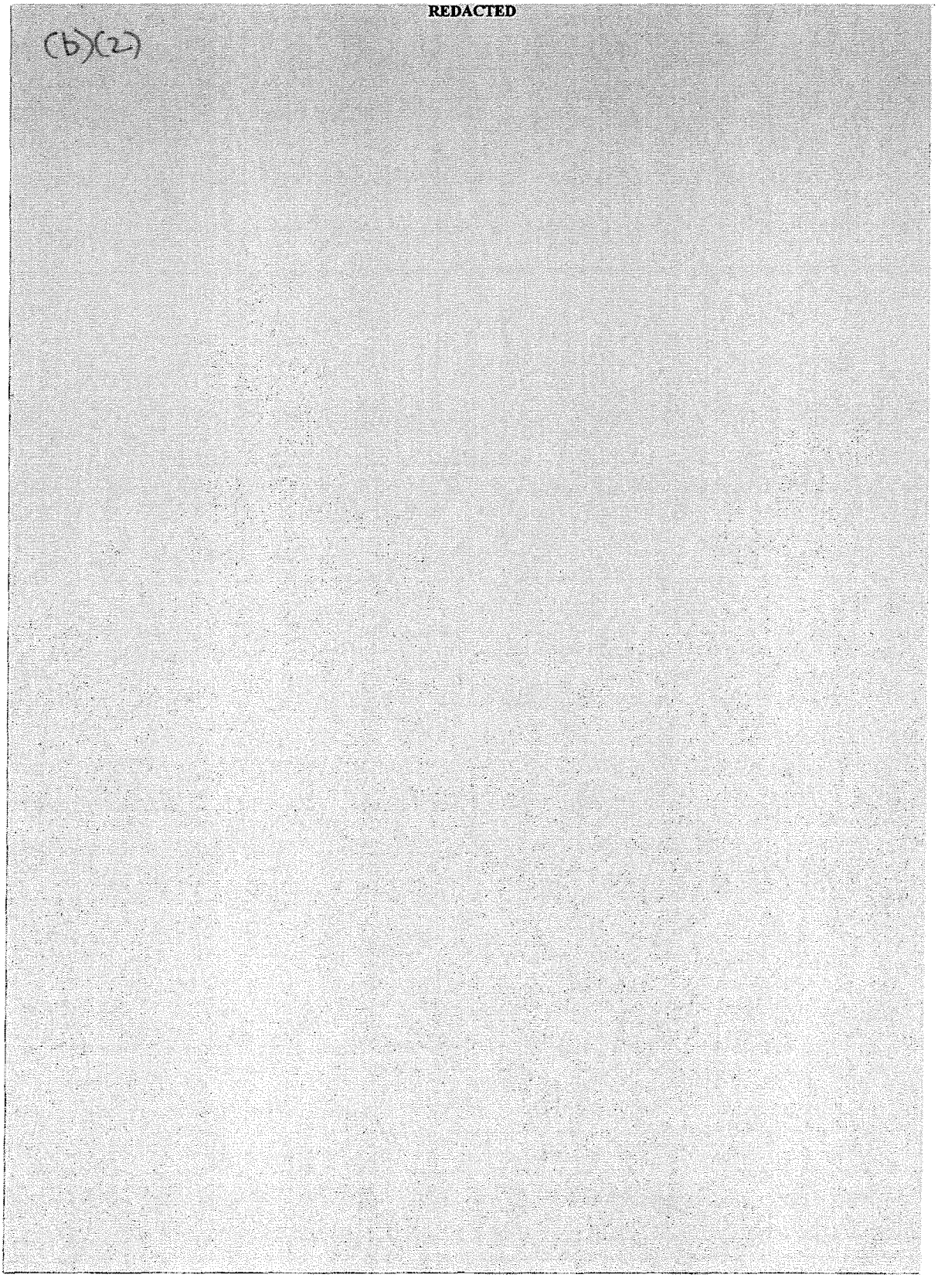

REDACTED
(b)(2)

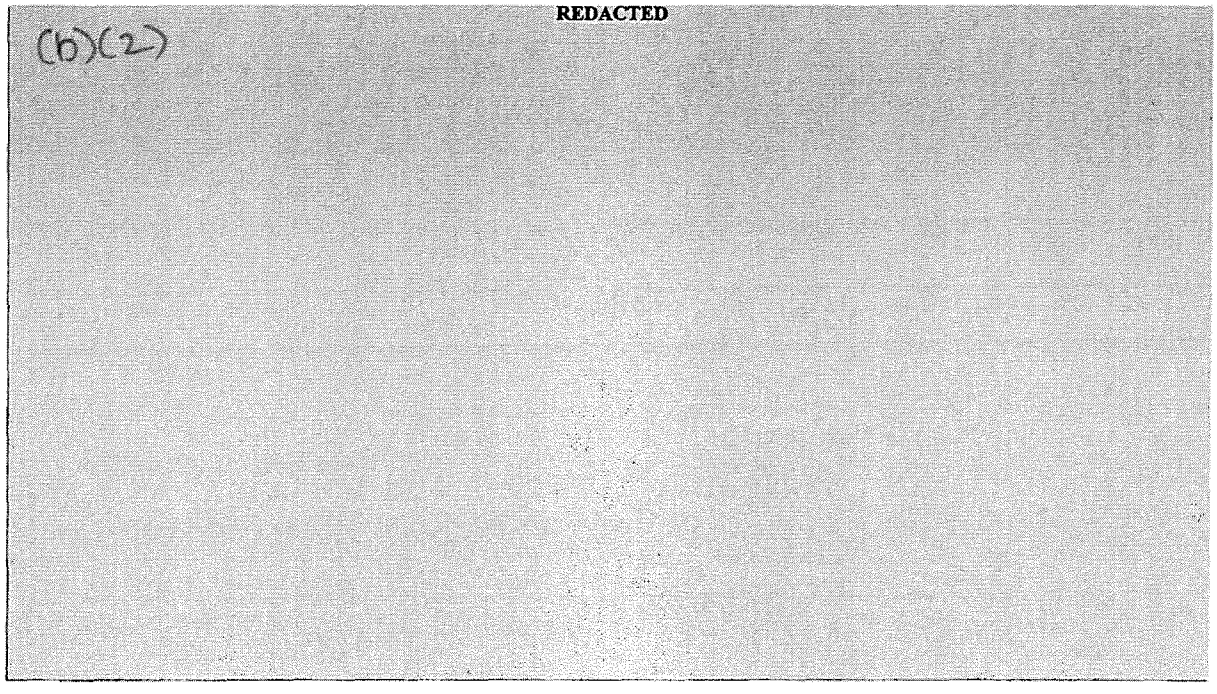

REDACTED
(b)(2)


REDACTED
(b)(2)

REDACTED

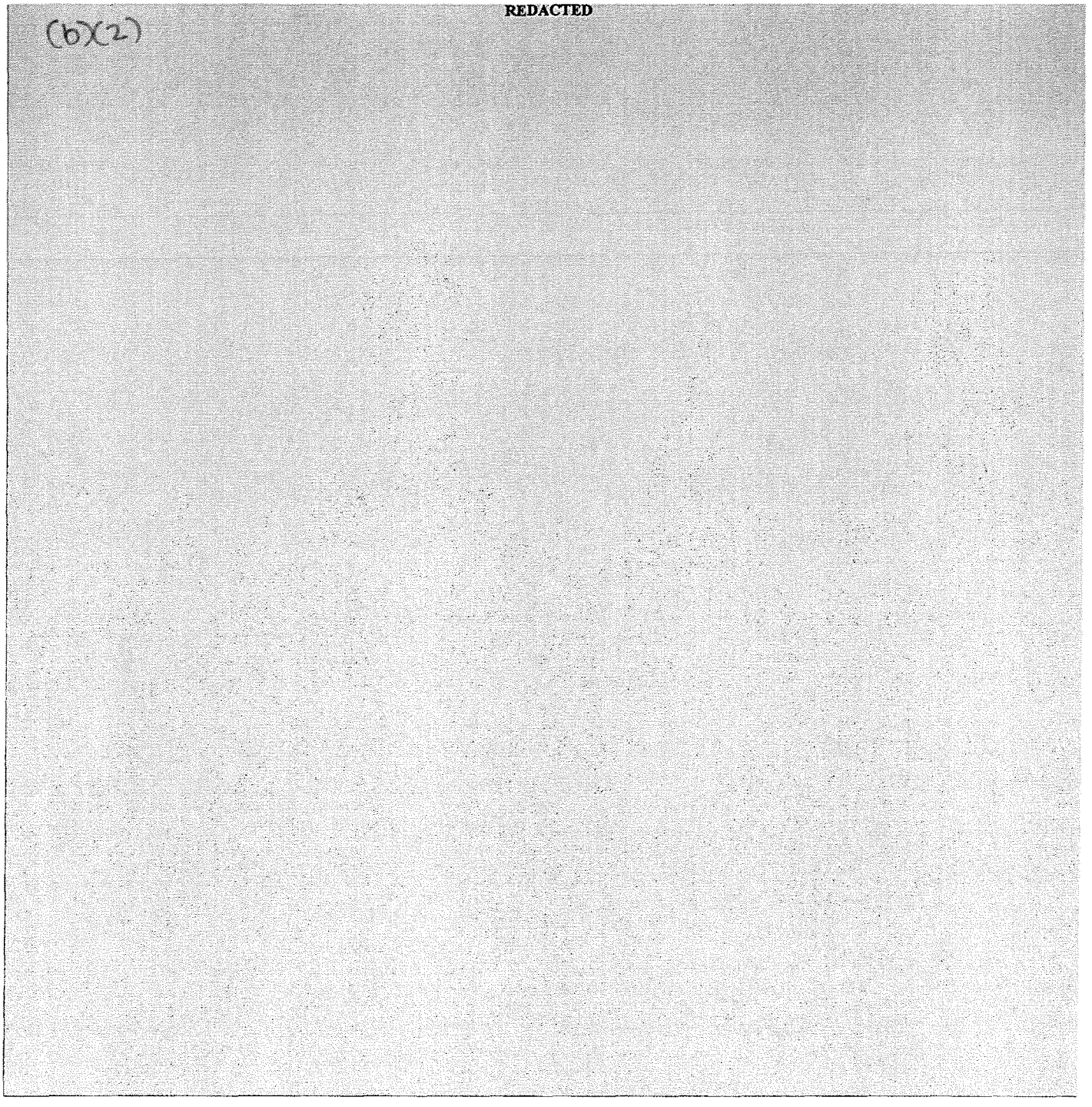
(b)(2)




REDACTED
(b)(2)

REDACTED

(b)(2)



(b)(2)

REDACTED

REDACTED

(b)(2)

8.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

The FTC security environment is robust and [redacted]

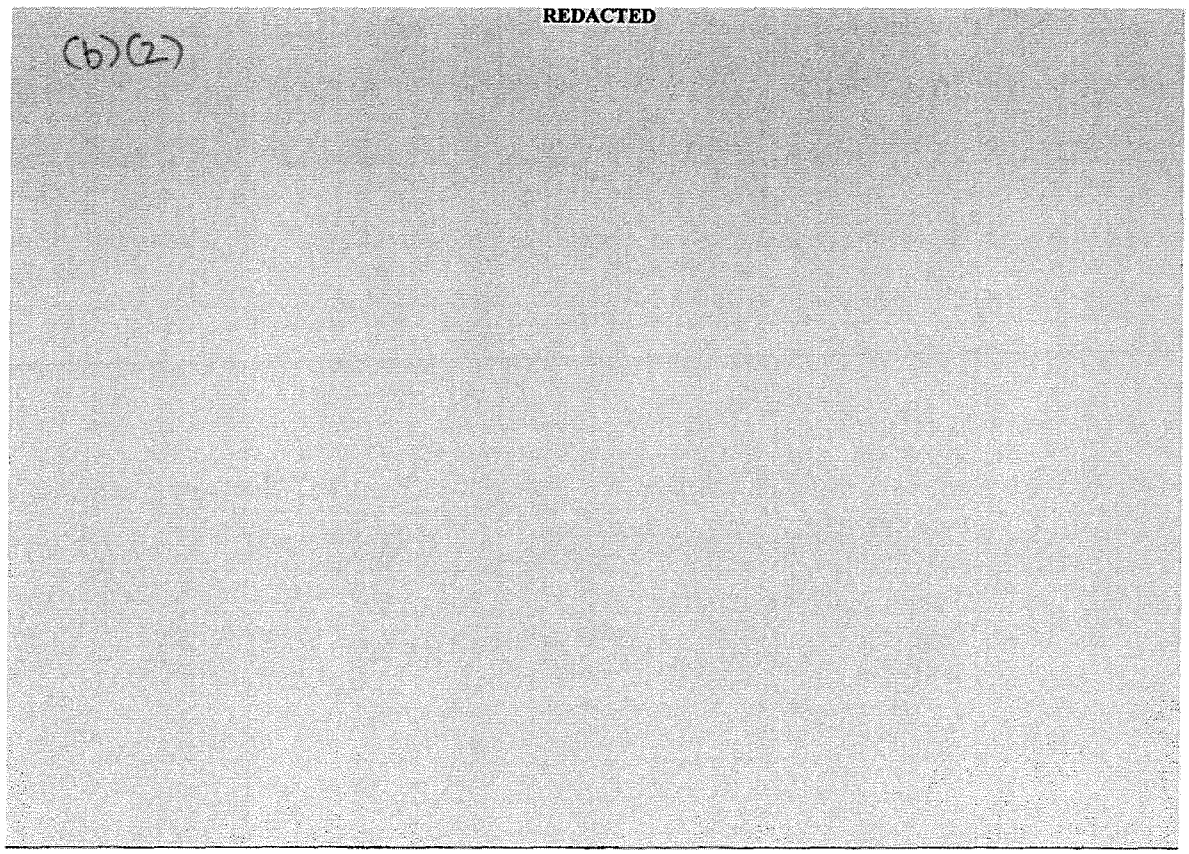
REDACTED

RED.

(b)(2)

REDACTED

(b)(2)


REDACTED
(b)(2)