



OFFICE OF THE  
INSPECTOR GENERAL

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

June 6, 2018

MEMORANDUM TO: Victor M. McCree  
Executive Director for Operations

FROM: Dr. Brett M. Baker /RA/  
Assistant Inspector General for Audits

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION OFFICE OF  
THE INSPECTOR GENERAL EXTERNAL VULNERABILITY  
ASSESSMENT AND PENETRATION TEST (OIG-18-A-14)

The Office of the Inspector General (OIG) conducted a vulnerability assessment and penetration testing of external Internet systems on the NRC computer network. OIG found that, overall, the external NRC perimeter and its Web applications responded well to testing conditions and NRC implemented several good practices. The testing team identified (b)(5) (b)(7)(F) Therefore, OIG makes 1 recommendation, to remediate the identified vulnerabilities in the findings matrix.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this report. Actions taken or planned are subject to OIG followup as stated in Management Directives 6.1.

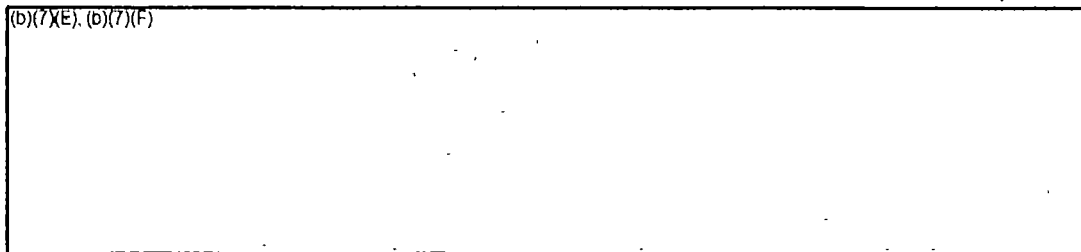
## Table of Contents

Abbreviations and Acronyms.....	ii-iii
1 Introduction .....	1
2 Scope.....	2
3 Methodology .....	4
3.1 Tools and Techniques .....	4
3.2 External Vulnerability Assessment and Penetration Testing .....	4
4 Vulnerabilities .....	7
4.1 Risk Ratings .....	7
5 Summary .....	12
5.1 Operational Findings Matrix .....	14
5.2 Recommendation .....	24
6 Comments for Management Consideration .....	24
Appendix A. Additional Details For High-Risk Findings .....	26

### List of Tables

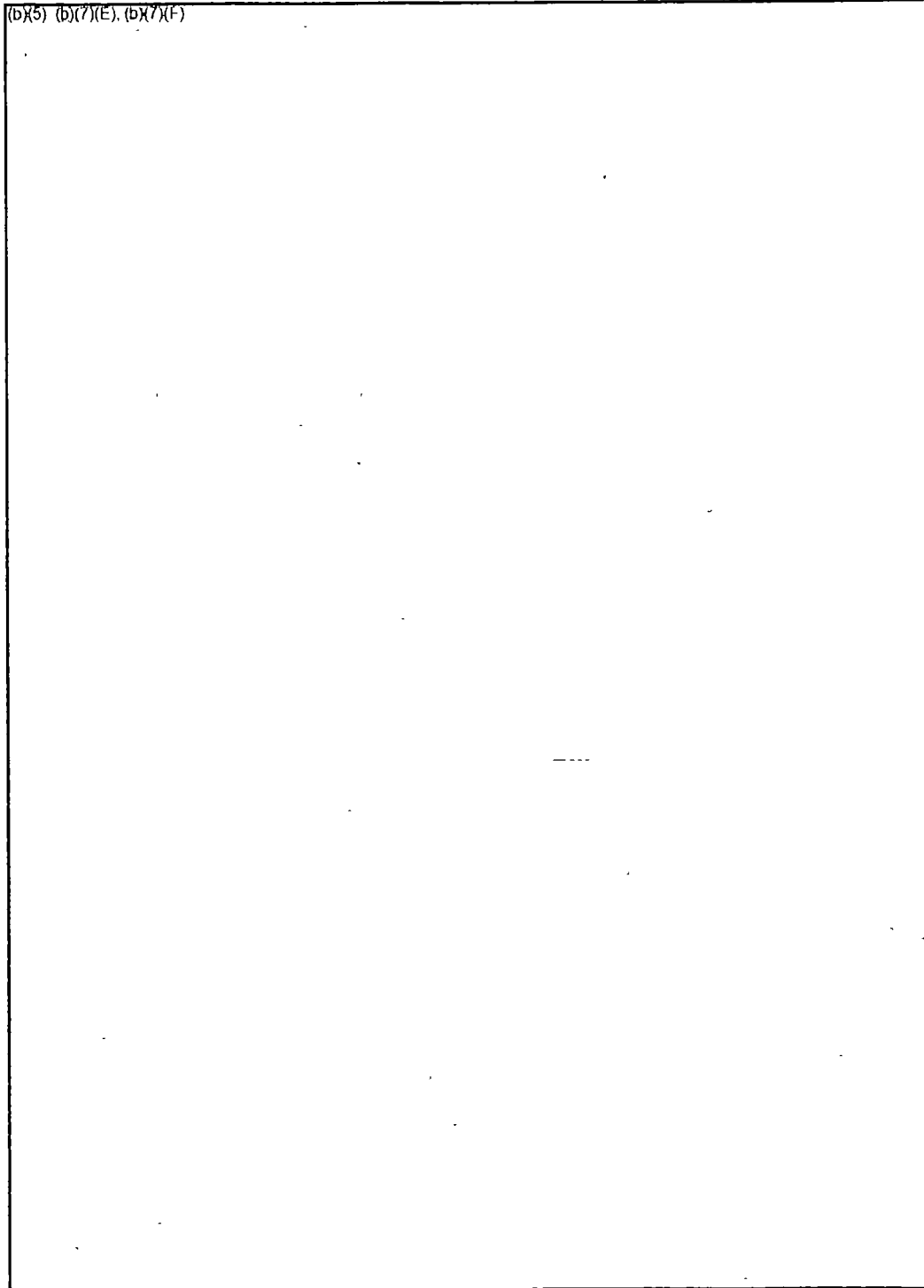
Table 1. Tools .....	4
Table 2. Summary of Findings by Risk Rating .....	7
Table 3. Vulnerability Rating Scale .....	8
Table 4. Regional Offices and TTC Results .....	12
Table 5. Findings Matrix.....	14

### List of Figures

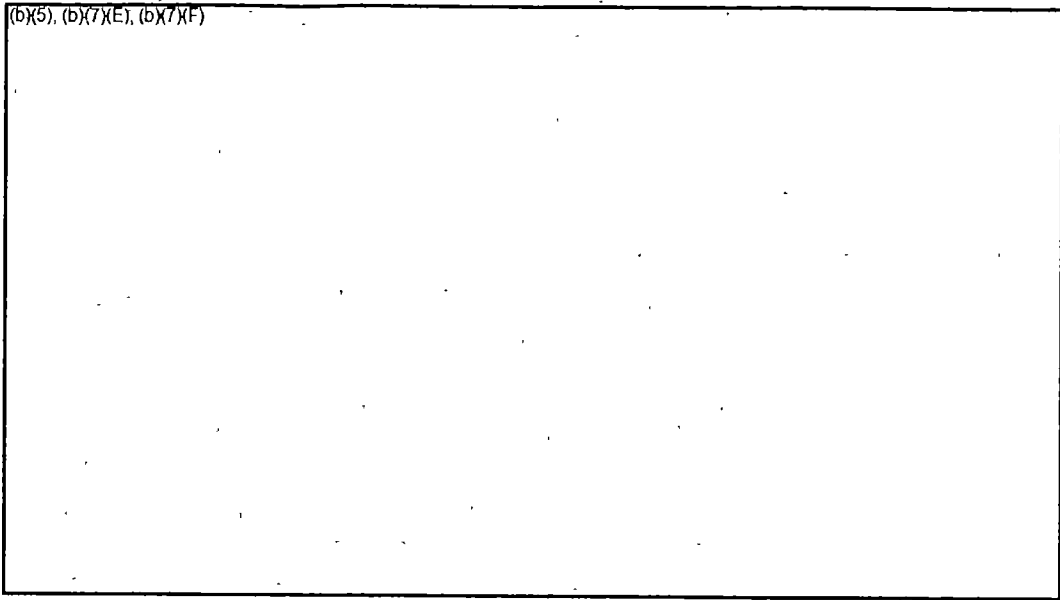


To Report Fraud, Waste, or Abuse .....	30
Comments and Suggestions .....	30

## Abbreviations and Acronyms



(b)(5), (b)(7)(E), (b)(7)(F)



## 1 Introduction

Richard S. Carson & Associates, Inc. (Carson Inc.) was tasked by the U.S. Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) to perform vulnerability assessment and penetration testing of external Internet systems on the NRC computer network. The testing was conducted from Carson Inc. Penetration Testing Lab facilities in Bethesda, MD, and the Washington, DC, metro area. The findings identified in this document represent vulnerabilities identified during the period of February 20 – March 23, 2018.

The goal of the testing was to verify the presence of network devices, identify vulnerabilities in external systems that could be exploited by external threats through the Internet, determine risk, and aid management in countering or mitigating the associated risks. The scope of the testing included vulnerability identification and exploitation by the testing team. The network devices included servers, routers, firewalls, and switches accessible from the Internet. The results of this testing should be used by NRC to measure progress in addressing network vulnerabilities from external sources.

Overall, the external NRC perimeter and its Web applications responded well to testing conditions and NRC implemented several good practices. The testing team identified (b)(5), (b)(7)(F)

(b)(7)(F)



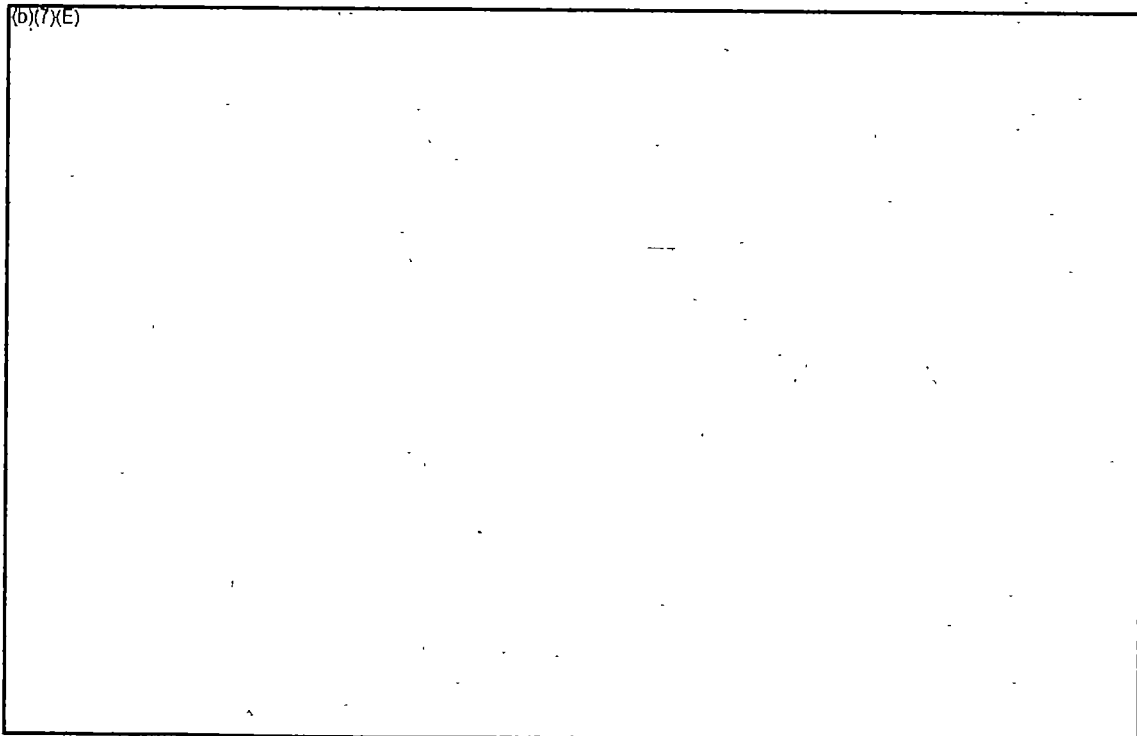
This report identifies the project scope, methodology, findings, and suggested remediation actions.

## 2 Scope

The external vulnerability assessment and penetration testing focused on NRC's Internet access points to include network devices, servers, and Web applications. The testing team used publicly available tools, proprietary methodologies, and diagnostic testing procedures to identify vulnerabilities and define areas for improvement. The testing team compared information system security practices with effective controls observed in the private industry to develop suggested remediation actions.

Multiple external Internet protocol (IP) ranges and Web application domains were provided by NRC OIG as in-scope for this assessment. No credentials were provided by NRC and all testing was performed unauthenticated.<sup>1</sup>

The testing team performed the security review with three phases:



<sup>1</sup> Unauthenticated testing means the testers did not try to enter credentials (e.g., user ID/password) for any Web sites that require them or to authenticate to servers in order to perform the testing.

(b)(7)(E)



The findings in this report based on data collected at the time of testing. The testing team used a risk-based approach to identify mission-critical vulnerable systems that can be used to access sensitive corporate information or compromise the reputation/mission and public trust of NRC. Carson Inc. does not provide any representation or warranty that every possible security issue has been identified as a result of these services or that NRC's systems are or will become free from unauthorized use or entry. In addition, any changes made to the system settings, services, or configurations after our data collection activity can significantly affect the validity of our findings and cannot be validated without re-testing and collecting system data to support identification of conditions.

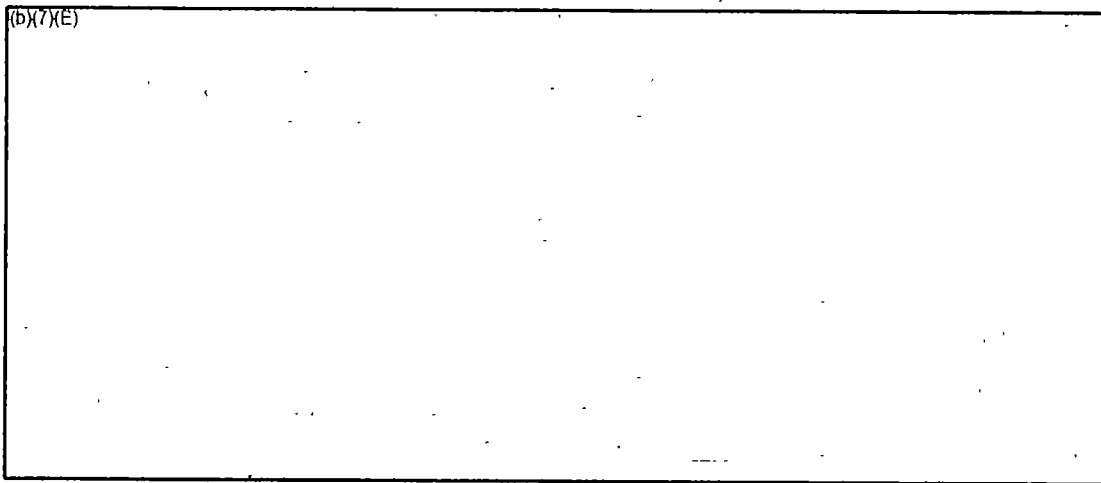
### 3 Methodology

The following section describes our primary focus and activities for the three main tasks.

#### 3.1 Tools and Techniques

The external vulnerability assessment and penetration test utilized a series of automated tools along with manual exploitation methods to identify security vulnerabilities and perform tests to exploit them actively in a non-harmful manner at the network and application layers against the above noted hosts.

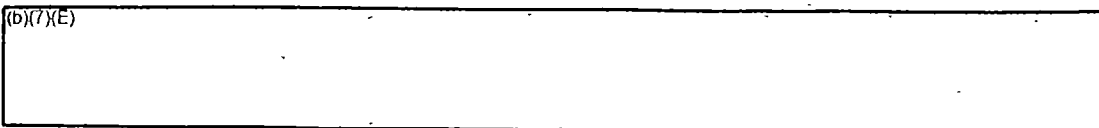
Standard tools utilized throughout the various assessment phases include



#### 3.2 External Vulnerability Assessment and Penetration Testing

Network vulnerability assessment and penetration testing was performed against NRC's Internet accessible devices. The testing team identified Internet systems and vulnerabilities associated with those systems using proprietary methodologies and network-based software tools.

The testing team performed a footprint analysis of the NRC Internet gateway and information servers to gain an understanding of the systems connected to the Internet. The footprint analysis and testing typically consists of the following:





- (b)(7)(E)
- 
- 
- 
- 
- 
- 
- 
- 
- 

The testing team also used penetration testing and vulnerability assessment methodologies to identify and exploit network-based vulnerabilities that could compromise Internet accessible systems. The scope of testing included the following:

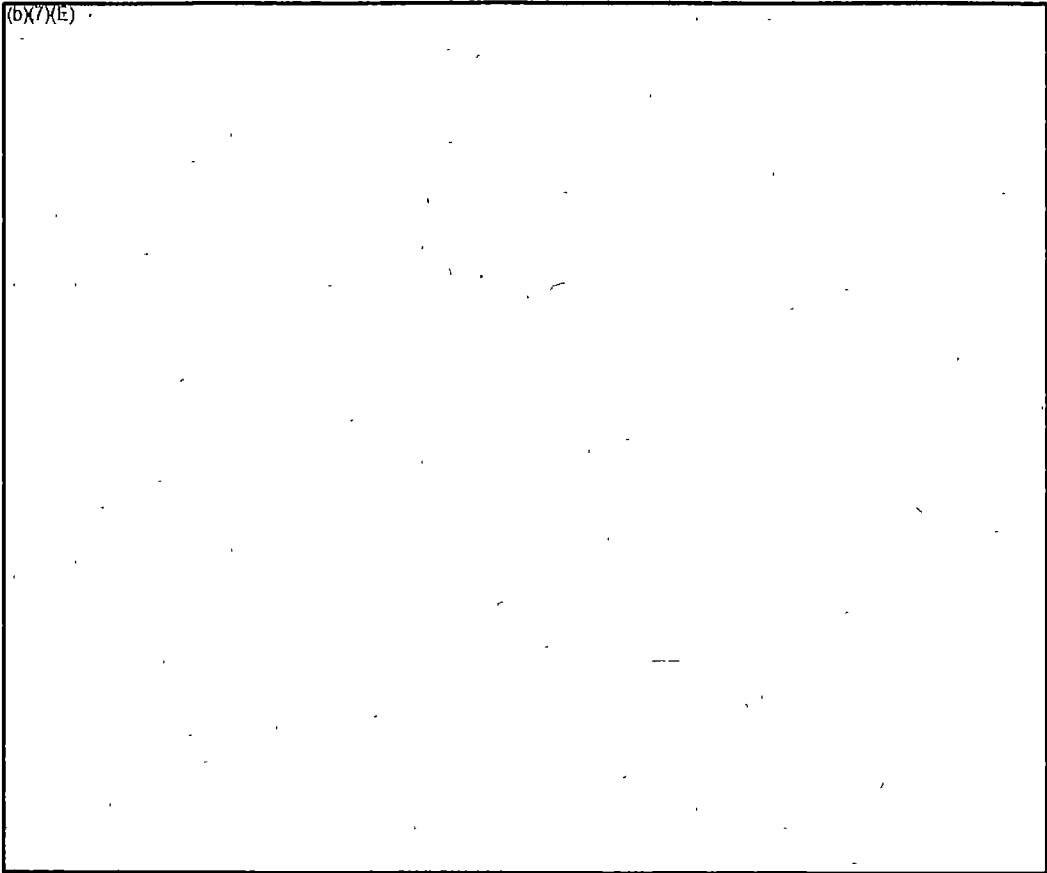
- (b)(7)(E)
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
-

(b)(7)(E)



For Web applications, the testing team assessed Web sites and Web services using automated tools in combination with manual testing. Depending on the Web application, assessment and exploiting encompassed testing for the following:

(b)(7)(E)

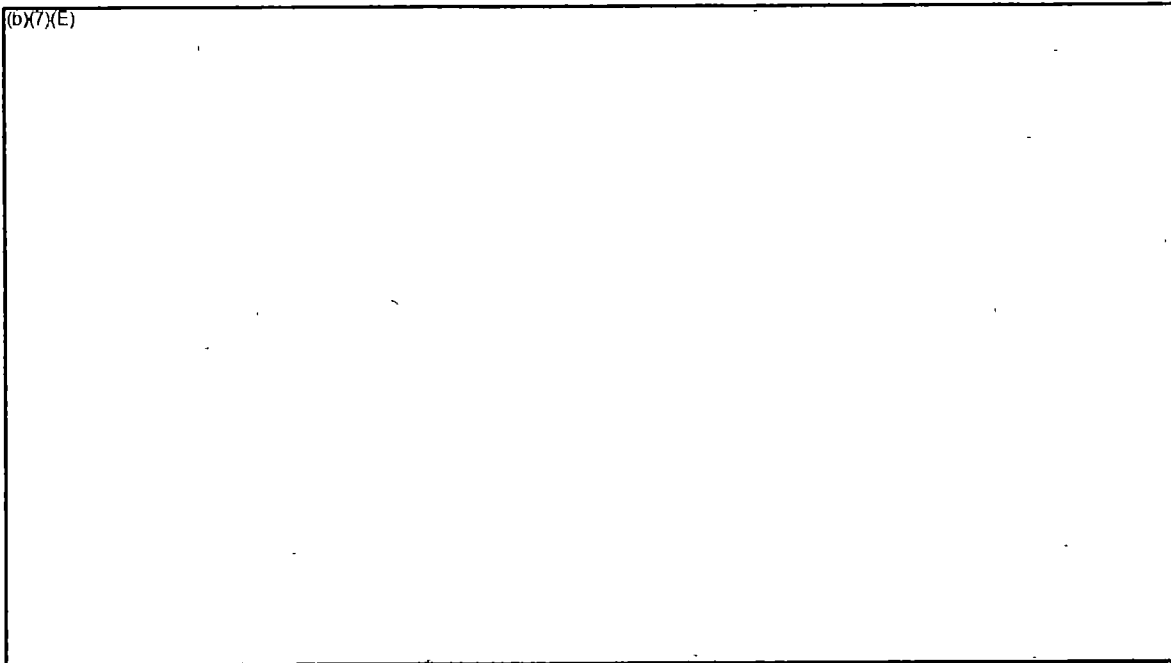


Network vulnerability assessment and penetration testing was performed against NRC's Internet-accessible devices. The testing team provided a listing of IP addresses in the Rules of Engagement, which were confirmed prior to testing for vulnerabilities using proprietary methodologies and network-based software tools.

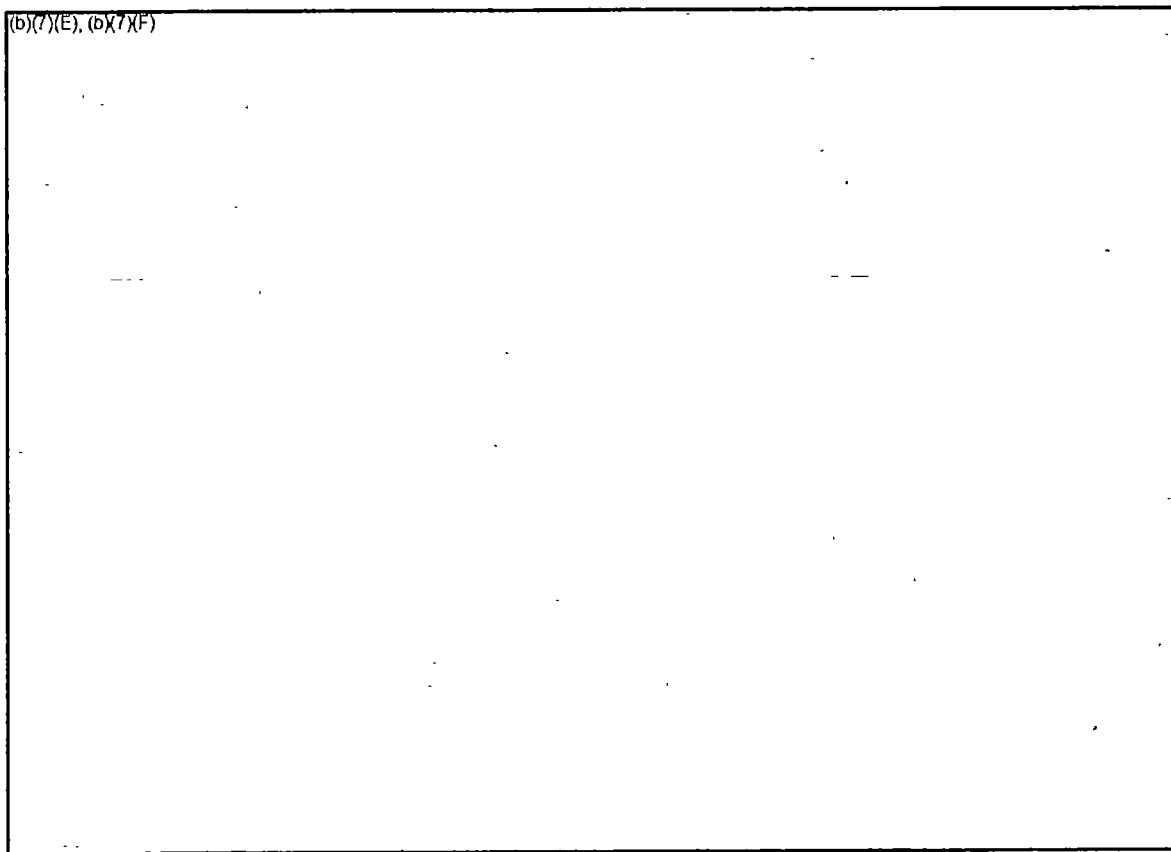
(b)(7)(E)



(b)(7)(E)



(b)(7)(E), (b)(7)(F)



The risk ratings are based on the testing team's risk determination and best practices in the industry. The risk impact ratings associated with each of the findings are based on the impact that the vulnerability would have on network security/network resources if exploited and the potential for being exploited. The findings been rated as high, medium, and low.

- A **critical-risk** finding indicates a severe condition that poses imminent risk to the environment, including unauthorized access to internal networks or systems that can be readily exploited under certain conditions.
- A **high-risk** finding indicates a condition that could directly result in unauthorized access to internal networks or systems.
- A **medium-risk** finding is a condition that would not provide for unauthorized access on its own, but does provide a significant capability or information that could be used in conjunction with other information or tools to gain unauthorized access to internal systems.
- A **low-risk** finding is a condition that does not directly lead to compromise of internal systems, but demonstrates an incomplete approach to security and provides supporting information—the complementary parts of an overall puzzle that an outsider could assemble in order to gain unauthorized access to internal systems.

**Table 3. Vulnerability Rating Scale**

Risk Rating	Description
<b>Critical/ High</b>	Critical implies activities/vulnerabilities that may immediately result in significant and/or permanent risk to company or client reputation or mission-critical operations.
	High includes activities/vulnerabilities that can be exploited by a skilled attacker to gain access to systems or sensitive information. This access could quickly evolve into a Critical risk based on the sensitivity of the systems or data being accessed.
	(b)(7)(E), (b)(7)(F)

**Table 3. Vulnerability Rating Scale (continued)**

Risk Rating	Description
<p align="center"><b>Critical/ High (continued)</b></p>	<ul style="list-style-type: none"> <li>• (b)(7)(E), (b)(7)(F)</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> </ul>
<p align="center"><b>Medium</b></p>	<p>This category may include one or more of the following:</p> <ul style="list-style-type: none"> <li>• (b)(7)(E), (b)(7)(F)</li> <li>•</li> <li>•</li> </ul>

**Table 3. Vulnerability Rating Scale (continued)**

Risk Rating	Description
<b>Medium (continued)</b>	• (b)(7)(E), (b)(7)(F)
	•
	•
	•
	•
	•
	•
	•
	•
	•

**Table 3. Vulnerability Rating Scale (continued)**

Risk Rating	Description
Low	This category may include one or more of the following: (b)(7)(E), (b)(7)(F) <ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li><li>•</li></ul>

It is the responsibility of NRC management to make risk management decisions addressing the vulnerabilities and their potentially realizable impacts on systems based on management assessments of the threats and the strength of the mitigating controls. The identification of the vulnerabilities in the report is independent of an analysis of the threat that outsiders exist to exploit it. This risk assessment assumes that real threats to NRC systems exist based on our knowledge of hacker practices and case history related to attacks by insiders. We believe a proactive security environment assumes that threat agents do exist.

(b)(5), (b)(7)(E), (b)(7)(F)

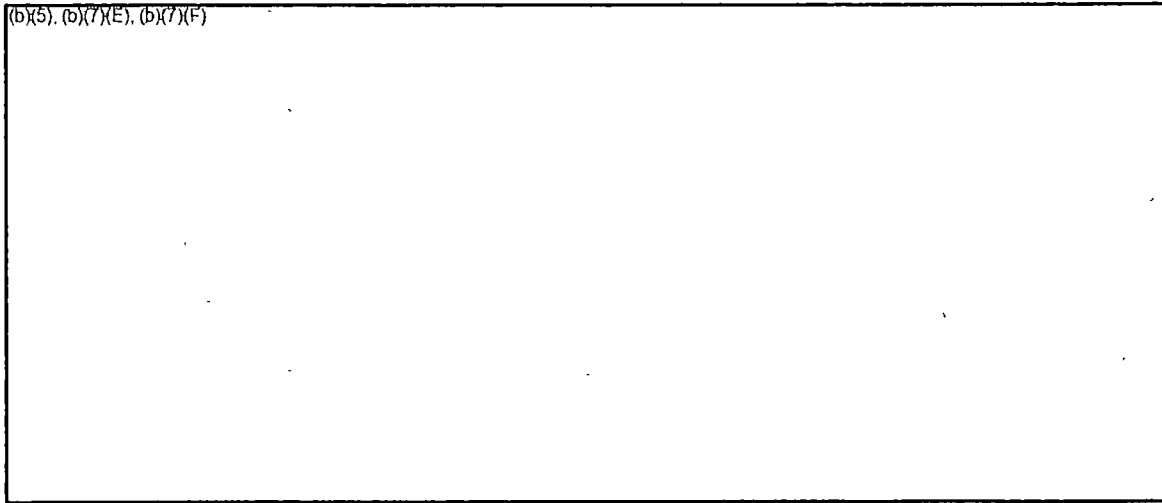
(b)(5), (b)(7)(E), (b)(7)(F)

**5 Summary**

(b)(5), (b)(7)(E), (b)(7)(F)

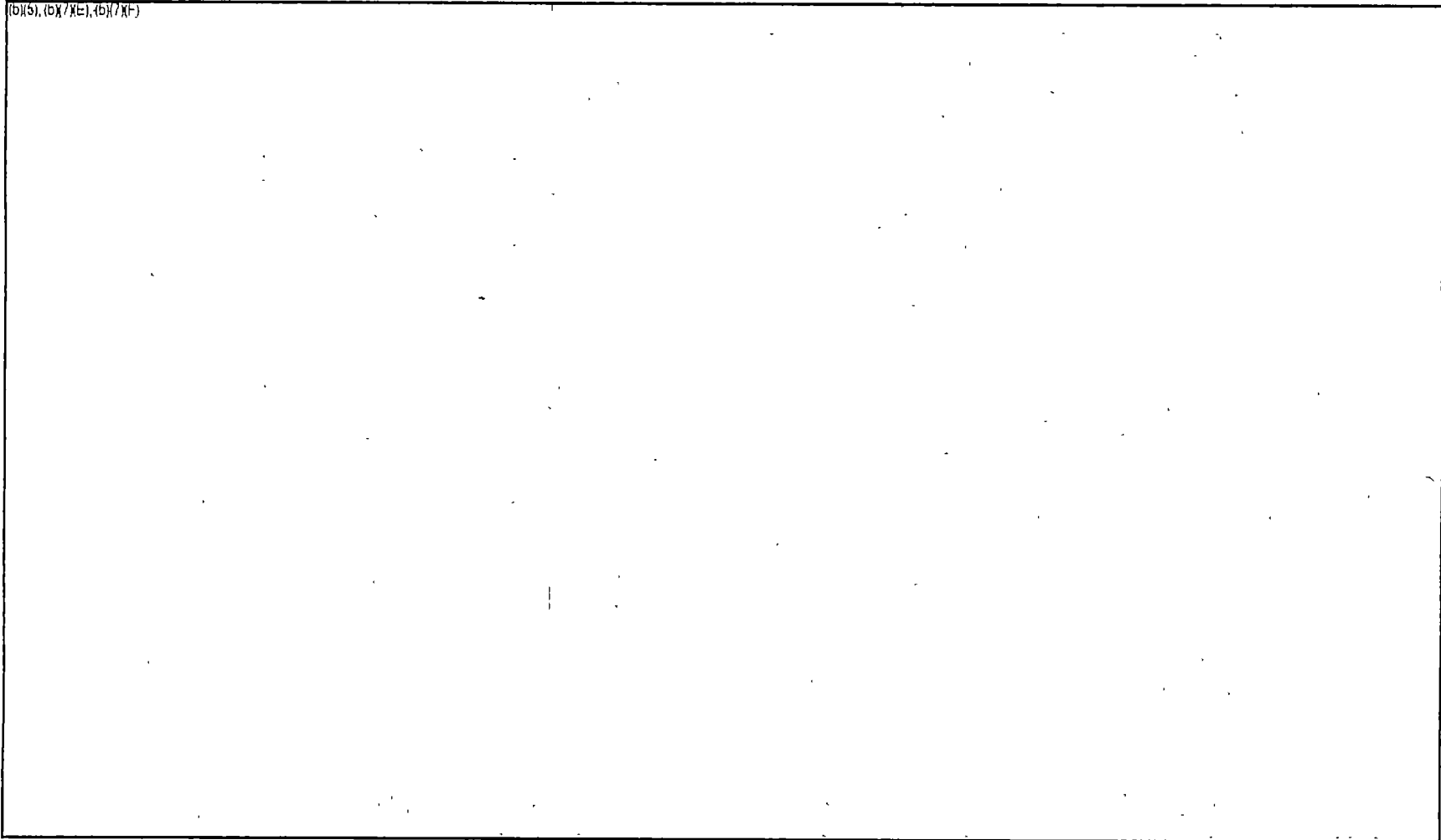


(b)(5), (b)(7)(E), (b)(7)(F)



5.1 Operational Findings Matrix

(b)(5), (b)(7)(E), (b)(7)(F)





(b)(5), (b)(7)(E), (b)(7)(F)



(DXS), (DX/RE), (DX/XF)



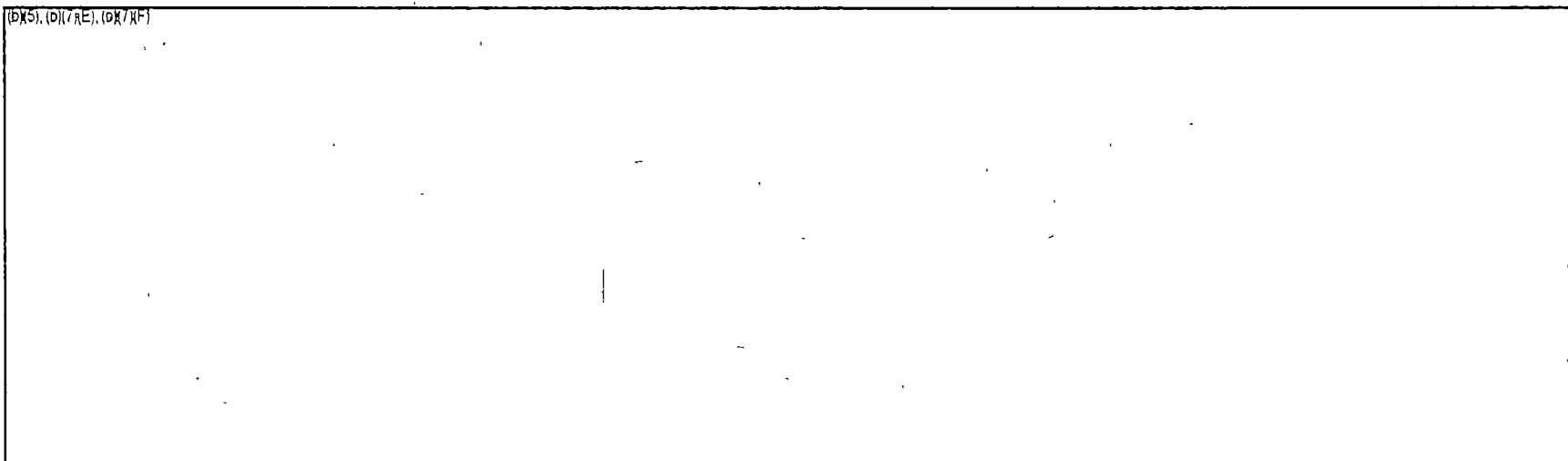








(b)(5), (D)(7)(E), (D)(7)(F)



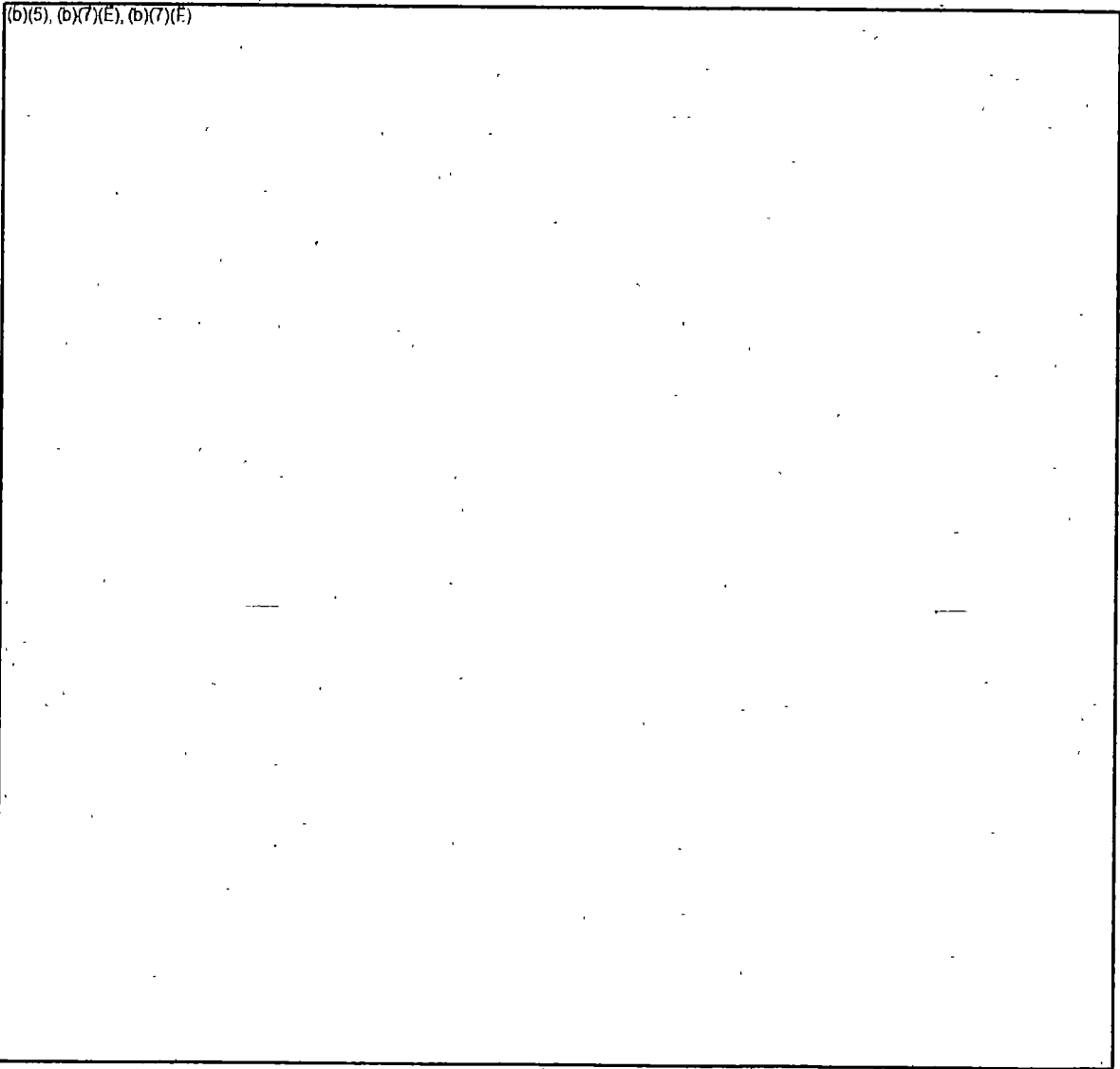
**5.2 Recommendation**

OIG recommends that the Executive Director for Operations:

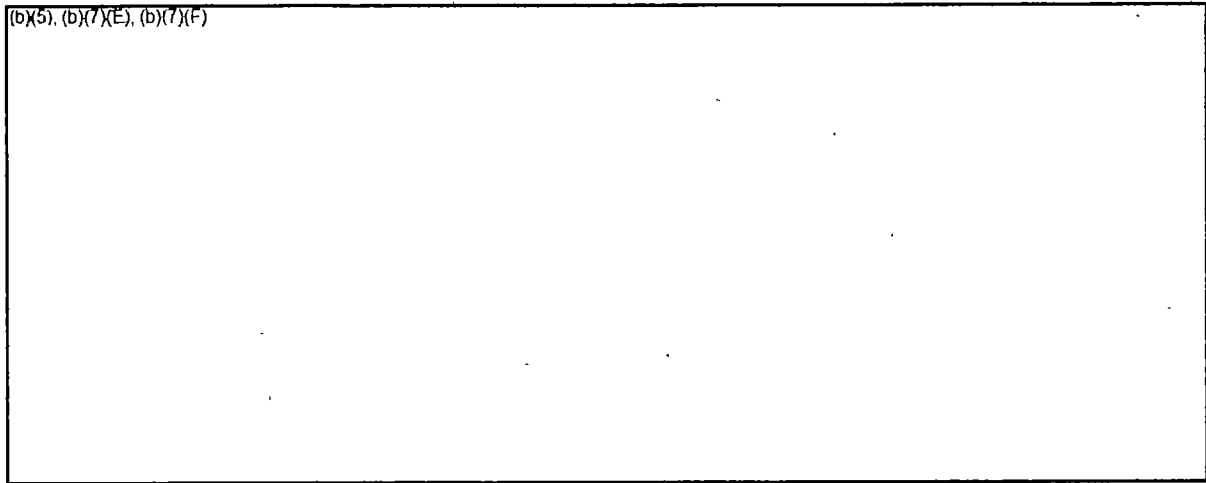
- 1: Remediate the identified vulnerabilities in the findings matrix.

**6 Comments for Management Consideration**

(b)(5), (b)(7)(E), (b)(7)(F)



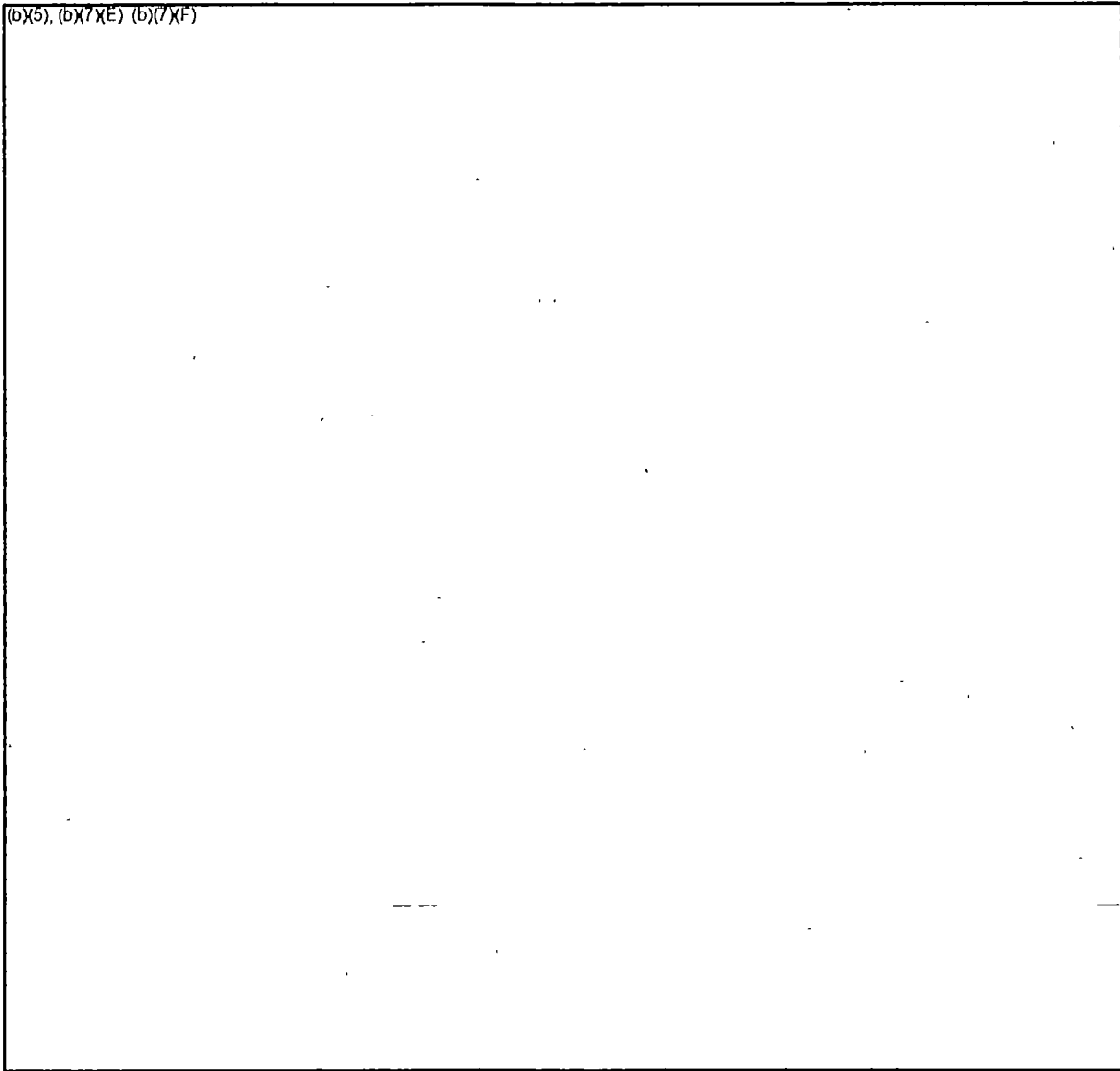
(b)(5), (b)(7)(E), (b)(7)(F)



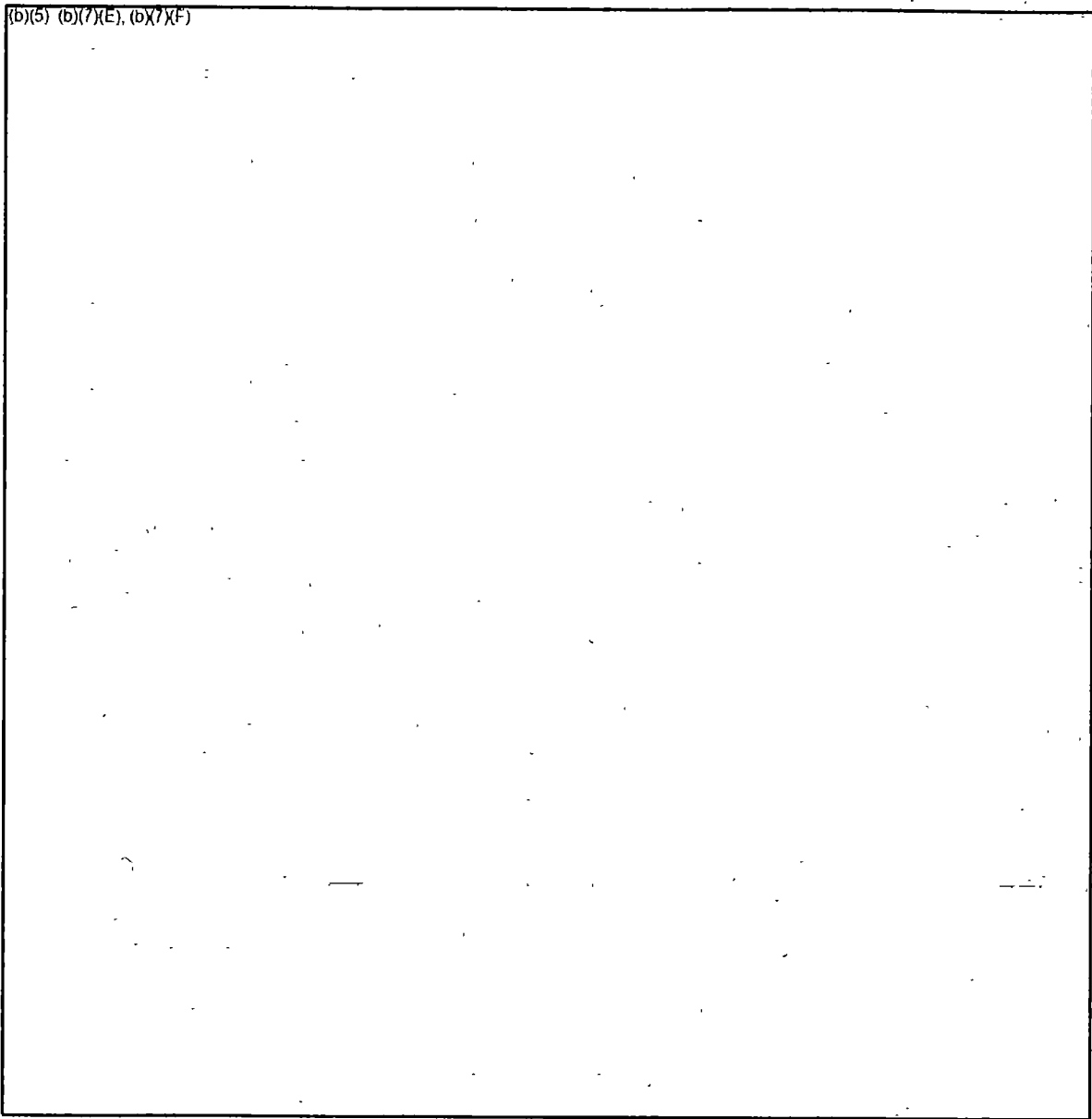
(b)(5) (b)(7)(E), (b)(7)(F)



(b)(5), (b)(7)(E), (b)(7)(F)

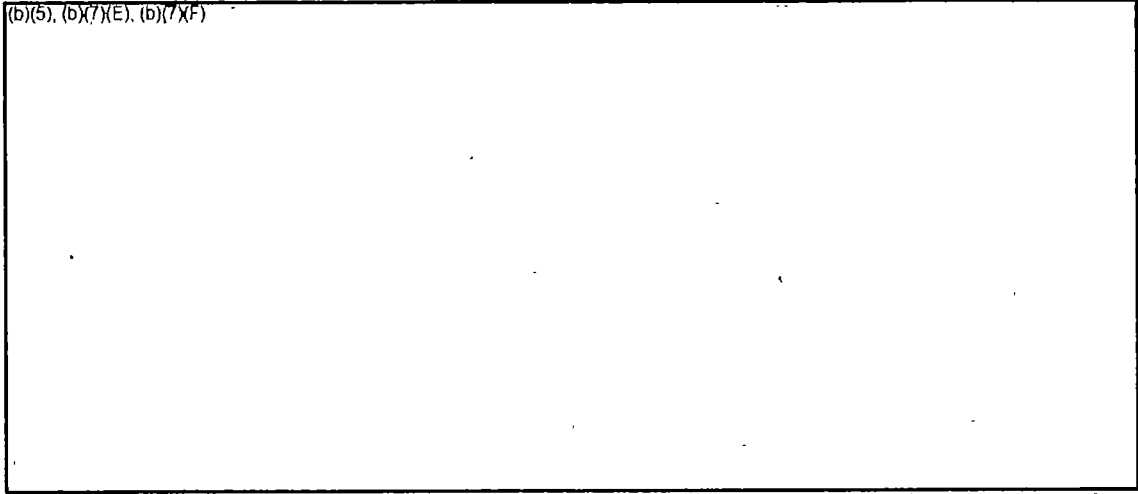


(b)(5) (b)(7)(E), (b)(7)(F)





(b)(5), (b)(7)(E), (b)(7)(F)



---

**TO REPORT FRAUD, WASTE, OR ABUSE**

---

**Please Contact:**

Email: Online Form

Telephone: 1-800-233-3497

TDD 7-1-1, or 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission  
Office of the Inspector General  
Hotline Program  
Mail Stop O5-E13  
11555 Rockville Pike  
Rockville, MD 20852

---

**COMMENTS AND SUGGESTIONS**

---

If you wish to provide comments on this report, please email OIG using this [link](#).

In addition, if you have suggestions for future OIG audits, please provide them using this [link](#).