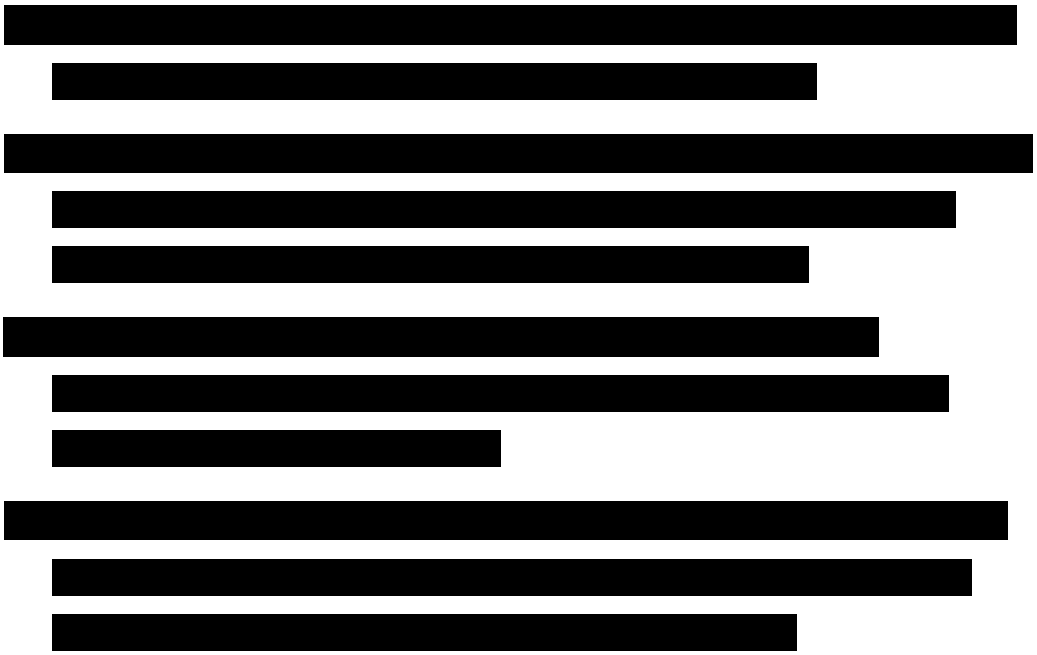
VOLUME 1, SECTION 5.6:

INCIDENT RESPONSE SERVICE

5.6 INCIDENT RESPONSE SERVICE (INRS) [C.2.10.5]

The Level 3 Team's Incident Response Service (INRS) will meet or exceed the Government's requirements for INRS, as defined in RFP Section C.2.10.5. This section provides a description of this service offering followed by responses to the specific requirements listed in RFP Section L.34.1.6.4, as they apply to this service.

The Level 3 INRS will provide agencies with an incident response plan that prepares for and minimizes the effects of an information security breach. Our Incident Response Team will formulate a comprehensive, customized course-of-action to immediately stop attacks in progress, minimize the impact of the breach, gather evidence, install remediation solutions and perform detailed forensics to curtail losses without shutting down mission-critical operations. Features of our INRS are listed below.



The Level 3 responses to the requirements in Table J.9.1.1.2 (b) Technical Stipulated Requirements for Optional IP Based Services are located in the Networx Hosting Center (NHC).

5.6.3 Service Requirements [C.2.10.5.1]

The Level 3 INRS fulfills the mandatory service requirements defined in RFP Section C.2.10.5.1. This section demonstrates our capabilities in the following areas:

- Standards
- Connectivity
- Technical Capabilities
- Features
- Interfaces

5.6.3.1 STANDARDS [C.2.10.5.1.2]

The Level 3 INRS will comply with the required standards as delineated in RFP Section C.2.10.5.1.2. Members of our team are active in numerous industry forums and working groups, which demonstrates our commitment to implementing future standards as technologies are developed and standards are defined and become commercially available. Our memberships include:

- Network Service Provider Security Association (NSP-Sec)
- International Systems Security Association (ISSA)
- VoIP Security Association (VOIPSA)
- Intrusion Detection Systems Consortium
- National Infrastructure Advisory Council (NIAC)

- Department of Homeland Security (DHS)
- National Institute of Standards and Technology (NIST)
- National Information Assurance Partnership (NIAP)
- Federal Bureau of Investigation (FBI)
- National Association of State Chief Information Officers (NASCIO)
- Information Technology - Information Sharing and Analysis Center (IT-ISAC)
- Open Security Evaluation Criteria (OSEC)
- Intrusion Detection Exchange Format Working Group (IDWG)

5.6.3.2 CONNECTIVITY [C.2.10.5.1.3]

Level 3 is a Tier 1 Internet Service Provider. Our INRS offering meets the connectivity requirements listed RFP Section C.2.10.5.1.3.

5.6.3.3 TECHNICAL CAPABILITIES [C.2.10.5.1.4]

5.6.3.3.1 Review the Agency's Security Infrastructure and Develop the Appropriate Strategic Plans

Based on a review of the agency's security infrastructure, the Level 3 Team will work with the agency to develop strategic plans that detail the incident response process, identify internal resources, assign duties to team members, describe policies, define severity levels, list escalation chains and specify emergency/recovery procedures.

[redacted] Level 3 will conduct an on-site work session with the members of the agency's computer security incident response team. These sessions will be intended to advise and assist the agency in the development and implementation of appropriate controls and procedures to prepare the

agency for a security incident, to educate agency staff on the topics of incident response and management, and to foster a stronger working relationship between Level 3's Emergency Response Team and the agency's computer security incident response personnel.

Work sessions can be conducted as seminars, interactive workshops, or one-on-one sessions, depending on the tasks to be accomplished. Work sessions may cover a variety of topics, including, but not limited to:

[redacted]

5.6.3.3.2 Provide Effective Incident Response Support on a [redacted] Basis

[redacted]

5.6.3.3.3 Provide Incident Analysis and Assessment to Determine Scope and Impact of Incidents

[redacted]

[redacted]

5.6.3.3.4 Coordinate with the Agency to Handle Potential Security Incidents According to the Appropriate Response Procedures

Once an emergency has been declared, our Incident Response team will work with the agency's Computer Emergency Response Team (CERT) to initiate the emergency response procedures. We will follow the agency's procedures and plan to ensure the incident is handled accordingly.

5.6.3.3.5 Provide Countermeasures to Contain the Security Incident, Limit its Spread, and Protect Internal Systems

If the security event is a true emergency and additional assistance from the CERT is requested, [redacted] Our security experts will follow a thorough incident response methodology, including:

[redacted]

5.6.3.3.6 Recommend the Fixes Necessary to Eliminate Identified Vulnerabilities, and the Appropriate Procedures to Guard Against Future Attacks

As stated above, Level 3 will provide recommendations and assistance to agencies to implement the necessary fixes to make sure that your computer systems and networks are protected from future occurrences of the identified vulnerabilities.

5.6.3.3.7 Provide the Agency with Secure Web Access to Incident Analysis Findings and Recommendations

For [redacted], Level 3 has developed [redacted] portal, which is based on the same platform as and adheres to the Government's intranet policy for design, operations, security, navigation, search, content architecture, and content management. [redacted]

5.6.3.3.8 Assist the Agency in Containing the Damage and Restoring Affected Systems to Their Normal Operational State

Level 3 will assist the agency in containing the damage and restoring the affected systems to their normal operation state. The stages of support include:

[redacted]

5.6.3.3.9 Assist the Agency in Testing Restored Systems to Ensure that Identified Vulnerabilities Have Been Corrected

As part of the [redacted] of incident response, Level 3 will assist the agency in testing restored systems to ensure the identified vulnerabilities have been corrected. Level 3 will work with the agency to make sure any affected computer system or network is returned to normal operation.

5.6.3.3.10 Provide Dedicated Support Until Resolution of the Problem

This requirement is satisfied in the response to Section 5.1.3.1.

5.6.3.3.11. Provide Post-Incident Investigative and Forensics Services

[redacted]

The individuals in this group will provide the following support to agencies:

[redacted]

[redacted]

5.6.3.3.12 Provide Telephone Support to the Agency, as Required

Agencies will have [redacted] telephone access to a Level 3 [redacted] via the agency-Dedicated Help Desk function described in Section 5.1.3.1 of this proposal volume.

[redacted]

5.6.3.3.13 Deploy Cyber Security Personnel to Agency Sites to Handle [redacted]

The Level 3 Incident Response Service (INRS) provides access to cyber security personnel [redacted], including holidays.

Whenever possible, such support will be provided remotely via the telephone and the Internet. Depending on the severity of the event, however, Level 3's response team will travel onsite to help respond. This offering is

[redacted] including holidays. We have personnel located throughout the United States. The dispersion of staff allows us to have team members on the ground, responding to an incident, typically within [redacted]

5.6.3.3.14 Provide Security Awareness Training to Agency Personnel as Required

[redacted]

5.6.3.4 FEATURES [C.2.10.5.2]

RFP Section C.2.10.5.2 specifies no features for INRS.

5.6.3.5 INTERFACES [C.2.10.5.3]

In compliance with RFP Section C.2.10.5.3, Incident Response Service analyses and recommendations will be accessible online through Level 3's secure [redacted] portal. This portal is a complete, web-enabled, self-service application that provides instant desktop access to an entire host of business performance metrics that empower an agency to manage its

network. The [redacted] portal gives Government customers direct access to the systems used by Level 3 internal staff.

5.6.4 Performance Metrics [C.2.10.5.4.1]

In accordance with RFP Section C.2.10.5.4.1, Level 3 will provide the performance metrics shown in [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]

[redacted]

5.6.5 Proposed Performance Improvements

Level 3 does not intend to exceed the AQLs in the KPIs at this time but would like to reserve the ability to do so with performance improvements that may be attained through the introduction of new technology. Level 3 believes in continuous improvement and will always strive to provide the highest quality services available.

5.6.6 Experience Delivering INRS

Managed Security Services is a core offering of both Level 3 and our partner [redacted] Details are provided in Section 5.1.3.4 of this proposal volume.

Our [redacted] has been providing INRS for more than [redacted] Every member of the [redacted] team is experienced in computer security incident response, having responded to [redacted] actual incidents. This track record has exposed our team to a wider variety of systems, network configurations, and attack methods than any single customer's team. In many cases, an incident that is new and unheard of to an agency will be familiar to our experts.

5.6.7 Monitoring and Measuring KPIs and AQLs

The Level 3[redacted] will monitor all Networx services provided using our IP backbone. Section 3.1.2.2 of this proposal volume describes the monitoring tools used by this organization that will allow for comprehensive visibility of numerous network elements and the ability to accurately measure AQLs for the applicable KPIs.

[redacted]

5.6.8 Optional Service Impact on Network Architecture

The INRS proposed by Level 3 will have no impact on the network architecture. There may be recommendations made as a result of an individual incident response. These changes would be made to improve the security of the network architecture and avoid any further security breaches.

5.6.9 NS/EP Functional Requirements

Section 2.5 of this proposal volume addresses how NS/EP requirements will be met for Networx services.

5.6.10 National Capital Region Service

Section 2.5.3 of this proposal volume discusses this topic in detail for all of Level 3's proposed services.

5.6.11 Meeting Section 508 Provisions

Reports generated as a result of an incident response engagement will be posted on the (3)Enterprise portal. The customer portal meets most of the requirements outlined in Section 508. The Section 508 requirements that are not met today can be met, rather easily, through simple modifications to the portal. Level 3 is committed to making these changes, should they be necessary.

In compliance with Section C.6.4 of the Networx RFP, Level 3 has prepared for a Voluntary Product Assessment Template (VPAT) for INRS and supporting documentation for Section 508, Subpart B, Technical Standards, paragraph 1194.22, Web-based Intranet and Internet Information and Applications. This data is provided in Section 2.5.5 of this Technical Volume.

5.6.12 Approach to INRS Technological Enhancements or Improvements

Level 3 is continually looking at ways to improve our incident response services. This includes using new tools, technologies and techniques to ensure we are providing our customer the highest level of service. As these new technologies become available, and tested, we will begin to incorporate their use into our service.

The approach to integrating any new technology would include the

[redacted]