6.2.2 INCIDENT RESPONSE SERVICE (INRS) (L.34.1.6.4, M.2.1.3)

Qwest Team INRS provides Agencies with a proven, reliable set of people, processes, and tools to effectively prepare for and respond to computer security incidents, all too common in today's Internet-connected environment.

Qwest has teamed [redacted] to provide Incident Response Service (INRS) to Agencies to fulfill the requirements of the RFP.

A computer security incident is defined as an adverse event in a computer system or network caused by an attempt to breach of a security mechanism or a failure of a security mechanism. Such incidents are becoming more common and their impact is far reaching. When faced with an incident, an organization must be able to respond quickly to protect both its own information and that of others affected. The Office of Management and Budget (OMB) Circular A-130 requires each Agency to be able to respond to security incidents and to share information concerning vulnerabilities and threats. Handling a security incident requires the six steps shown in [redacted]

[redacted] provides a closer look at these six steps as an example of our response to viruses.

Figure 6.2.2-1. Six Steps for Incident Response

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

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

[redacted]

The Security Operations Center (SOC) infrastructure is designed on best-of-breed technology and is modular for rapid expansion and transaction processing. Our Security Information Manager (SIM) is scalable to tens of thousands of log events per second, regardless of geographical location. The Qwest Team provides information security services to many Agencies as well as the financial, information technology, energy, aerospace, health, entertainment, and publishing industries. Qwest is set apart by the personalization and attention we give to each Agency. We understand that having a lead engineer assigned as a point of contact along with trained, cleared personnel delivering services provides peace of mind.

6.2.2.1 Reserved (L.34.1.6.4 (a))

6.2.2.2 Reserved (L.34.1.6.4 (b))

6.2.2.3 Technical Service Requirements (L.34.1.6.4 (c))

The Qwest Team's INRS provides Incident Response Capability (IRC) assessment, an incident tracking system, a mock-crisis management scenario, incident response support services, and on-site support. We offer IRC development, a successful process for minimizing incident impacts and exposures, and a core staff of recognized incident response experts. The Qwest Team's resources include world-class information protection laboratories, and worldwide deployment of proprietary, country-approved tools.

The Qwest Team can provide notification of threats to Agencies well in advance, protecting them from incidents because of our broad inter-Agency view. Examples of this support are:

- ***Fraud/Incident Support:*** The Qwest Team will provide expert, incident-specific support before, during, and after investigations of technology fraud and security incidents. We offer high-level expertise, customized solutions for various incidents, and focus on technical, human, and business assessments.
- ***Pre-Incident Planning and Preparation:*** We offer policy and procedures development and review, organizational assessments, education, and awareness training.
- ***During Incident:*** Services include incident handling and analysis, on-site incident response support and coordination, and, if appropriate, forensics and evidence collection.

- ***Post-Incident:*** This includes artifact handling, analysis and response, forensic analysis, reports, conclusions and recommendations, and aftermath assessment.

6.2.2.3.1 Satisfaction of INRS Capability Requirements (L.34.1.6.4 (c), C.2.10.5.1.4)

The Qwest Team's INRS offering meets the required capabilities as shown in ***Figure 6.2.2-3***. Qwest fully complies with all mandatory stipulated and narrative capability requirements for INRS. The text in Figure 6.2.2-3 provides the technical description required per L.34.1.6.4 (c) and does not limit or caveat Qwest's compliance in any way.

Figure 6.2.2-3. Qwest Team INRS Capabilities

Required INRS Capabilities	[redacted]
1. The contractor shall review the Agency's security infrastructure and develop the appropriate strategic plans in collaboration with the Agency. These plans shall detail the incident response process, identify internal resources, assign duties to team members, descr be policies, define severity levels, list escalation chains, and specify emergency/recovery procedures.	[redacted]
2. The contractor shall provide the Agency with effective incident response support on a 24x7x365.	[redacted]
3. The contractor shall provide incident analysis and assessment in order to determine the scope and impact of incidents.	[redacted]
4. The contractor shall coordinate with the Agency to handle potential security incidents according to the appropriate response procedures.	[redacted]
5. The contractor shall provide	[redacted]

Required INRS Capabilities	[redacted]
countermeasures to contain the security incident, limit its spread, and protect internal systems.	[redacted]
6. The contractor shall recommend the fixes necessary to eliminate identified vulnerabilities and the appropriate procedures to guard against future attacks.	[redacted]
7. The contractor shall provide the Agency with secure Web access to incident analysis findings and recommendations.	[redacted]
8. The contractor shall assist the Agency in containing the damage and restoring affected systems to their normal operational state.	[redacted]
9. The contractor shall assist the Agency in testing restored systems in order to ensure that identified vulnerabilities have been corrected.	[redacted]
10. The contractor shall provide dedicated support until resolution of the problem.	[redacted]
11. The contractor shall provide post-incident investigative and forensics services. This includes isolating the impacted area, capturing and collecting data, categorizing malicious or illegal events, and performing reconstruction analyses. The contractor shall handle and preserve the data collected according to sound scientific and evidence rules, as the information may serve as evidence in administrative actions and legal proceedings. The contractor shall trace the offenders and assist in prosecuting attackers, as required.	[redacted]
12. The contractor shall provide telephone support to the Agency, as required.	[redacted]
13. The contractor shall deploy cyber security personnel to Agency sites to handle security incidents, as necessary.	[redacted]
14. The contractor shall provide security awareness training to Agency personnel as required. This includes mock attack drills, emerging threats and vulnerabilities workshops, and	[redacted]

Required INRS Capabilities	[redacted]
new incident response tools and processes demonstrations. The frequency and nature of training activities may vary according to Agency needs.	[redacted]

6.2.2.3.2 Satisfaction of INRS Feature Requirements (L.34.1.6.4 (c), C.2.10.5.2)

There are no INRS Feature requirements under the RFP Section C.2.10.5.2.

6.2.2.3.3 Satisfaction of INRS Interface Requirements (L.34.1.6.4 (c), C.2.10.5.3)

All incident response analysis and recommendations will be available via secure access to the Qwest Control Networx Portal. Qwest fully complies with all mandatory stipulated and narrative interface requirements for INRS. The text above provides the technical description required per L.34.1.6.4 (c) and does not limit or caveat Qwest’s compliance in any way.

6.2.2.4 Achieving Quality of Service Goals (L.34.1.6.4 (d))

Our Incident Response Service performance metrics are shown in ***Figure 6.2.2-4***.

Figure 6.2.2-4. Qwest INRS Key Performance Indicators (KPIs)

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[redacted]
Response Time (Telephone)	Routine	Within 1 hour of the notification for a Low category incident	≤ 1 hour	[redacted]
		Within 15 minutes of the notification for a High category incident	≤ 15 minutes	[redacted]
Response Time (On-Site)	Routine	Within 36 hours of the notification for a Low category incident	≤ 36 hours	[redacted]
		Within 24 hours of the notification for a High category incident.	≤ 24 hours	[redacted]

The Qwest Team’s INRS meets all performance requirements. We have proven monitoring and measurement systems, procedures, and evaluation methods in place. The Government performance metrics are consistent with commercial standards, and we will meet each of these performance requirements by staffing our SOC 24x7x365. The Qwest Team has the necessary resources available to respond to incidents encountered by Agencies.

6.2.2.5 Proposed Service Enhancements (L.34.1.6.4 (e))

[redacted]

6.2.2.6 The Qwest Team Experience (L.34.1.6.4 (f))

The Qwest Team's INRS is an integral component of our Managed Security Service Provider (MSSP) offering and is unique in its capabilities and experience, because our service offerings extend beyond those of a typical MSSP. Our approach is to provide a customer-focused premium service that is vendor-and device-independent. This allows Agencies to retain their current infrastructure and also facilitates future upgrades and technology refreshments, providing our customers significant long-term benefits—and making us a trusted advisor. [redacted] Our experience is multi-dimensional; the MSS is enhanced by the availability of a large security organization that can support all of our security recommendations. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6.2.2.7 Approach to Performance Verification (L.34.1.6.4 (g))

All incident response reports are tracked in our [redacted] Trouble Ticket System. Reports are processed by analysts according to an established workflow, and response times are tracked for each report and event. Data to support the measurement of the Government-specified KPIs is collected on a continuous basis; computed statistics are made available to authorized Agency personnel [redacted] The raw data is collected through the INRS system, network, and availability monitoring tools, and through our customer change/problem tracking system.

6.2.2.8 Service Impact to Network Architecture (L.34.1.6.4 (h))

[redacted]

6.2.2.9 Approach to Satisfying NS/EP Requirements (L.34.1.6.4 (i))

As defined in RFP Section C.5.2.2.1, INRS is not a National Security and Emergency Preparedness (NS/EP) impacted service. Qwest's overall support of the NS/EP requirements can be found in Section 3.5.1 and our NS/EP plan can be found in Appendix 2 to the Technical Volume.

6.2.2.10 Approach to Assured Service in the National Capital Region (L.34.1.6.4 (j))

Qwest is currently a leading provider of network services in the National Capital Region (NCR) with robust network architecture to ensure service continuity in the event of significant facility failures. Qwest has, and will continue to engineer, critical services to meet the requirements of each Agency to eliminate single points of failure for their network services.

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. To meet this important requirement, Qwest has established Point-of-Presence (POP) diversity in the NCR. [redacted] Each of these gateways provides complete redundancy to access Qwest nationwide and international network capabilities as well as regional voice and data services. [redacted]

[redacted] Section 3.5.2 provides additional detail regarding our NCR infrastructure.

Qwest recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. This gives Qwest at least three regional fiber optic networks to use to ensure redundancy and survivability in the greater Washington D.C. area.

The Qwest Team has multiple SOCs that are geographically diverse and no MSS is dependent on assets located solely within the NCR region.

6.2.2.11 Approach to Meeting Section 508 Provisions (L.34.1.6.4 (k)

Qwest's initial approach to Section 508 provisions is to ensure that all Agency users are able to access all systems and services. To ensure this, the Qwest Control Networx Portal will be 508 compliant. The Qwest Control Networx Portal is the gateway to Qwest Networx support systems. The support systems for INRS are compliant with applicable accessibility standards in Subpart B. This Portal will serve as the primary conduit for daily status pertaining to ongoing projects and other service delivery activities for Agencies.

In addition, Qwest has enlisted a single toll-free number for 24x7x365 access: 1-866-GSA-NETWorx (1-866-472-6389). This toll-free number will allow domestic Agency users to have access to our Customer Support Office (CSO), which will also be 508 compliant—enabling accesses by email, fax, TDD, text messaging, or other methods as required. Qwest customer service support will be accessible around the clock for all Agency users, wherever they may be located.

The Qwest approach for ensuring that its products and services are 508 compliant is to go through the same rigorous testing and evaluation that all products and services go through before they are made available to the public. Qwest works with industry and specific assistive technology vendors to ensure that all of the Qwest products and services are 508 compliant. Section 3.5.3 provides further information regarding our compliance with Section 508 provisions.

6.2.2.12 Approach to Incorporating Technological Enhancements and Improvements (L.34.1.6.4 (l))

Qwest has a proven, mature process that enables us to envision, research, evaluate, engineer, deploy, and operate new or emerging services including INRS. Driven initially by the Chief Technology Office, Qwest evaluates new products and technologies for incorporation into the Qwest network, in partnership with Qwest Product Management.

[redacted]

[redacted]

[redacted]

Qwest's suppliers participate fully in this process. Qwest ensures compliance with suppliers by evaluating, testing, and certifying all emerging technology. The vendors on the Qwest Team are committed to driving new technologies and products. New technology, provided by suppliers, is driven through and implemented via NTSC process in order to standardize all new products and technologies we will present to Agencies.