6.6 INCIDENT RESPONSE MANAGEMENT SERVICES (INRS) (L.34.1.6)

Qwest 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.

A computer security incident is defined as an adverse event in a computer system or network caused by a failure of a security mechanism or an attempt to breach these mechanisms. Such incidents are becoming more common and their impact is far reaching. When faced with an incident, an organization should 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 six steps shown in ***Figure 6.6-1***.

Figure 6.6-2 provides a closer look at these six steps – as an example of our response to viruses.

Figure 6.6-1. Elements of the Qwest Incident Response Management Service

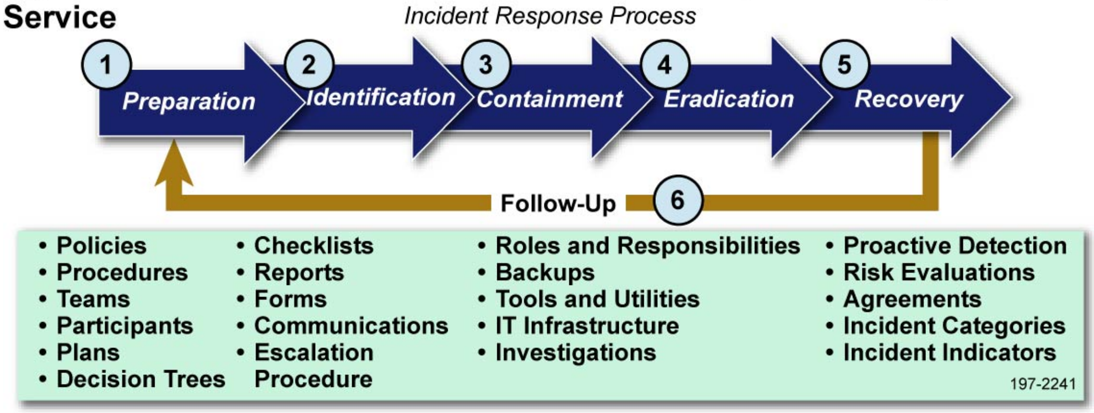


Figure 6.6-2. Six Steps for Incident Response

Steps	Activities Involved and Discussion
1. Preparation	• Assess impacts of viruses and containment efforts • Identify software or hardware needed for response • Determine types and number of personnel resources needed • Develop containment strategy, test it, and reassess its impact • Procure items and assign personnel resources identified in assessment phase
2. Identification	• Identify virus type and assess impact • Determine how virus is spread (ports, email, other) using tools such as sniffer traces and logs • Develop containment strategy to limit spread • Identify critical business users and systems, prioritize clean-up
3. Containment	• Quarantine and physically remove all potentially infected PCs from the network • Detect and remove virus • Apply OS software patch • Install/update virus software
4. Eradication	• Perform a virus scan via a bootable disk, install MS patch, install current virus protection software, and scan • Where possible, perform these procedures first on critical PCs • Perform quality assessment of each vulnerable PC to ensure that it is clean, protected, and ready to be put back into production
5. Recovery	• All PCs that have passed the Quality Assurance procedure are returned to production status and tested • Continue monitoring network traffic as warranted
6. Follow-Up	• Conduct follow-up analysis roundtable discussion • Document lessons learned, change preparation plans accordingly

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 is scalable to tens of thousands of log events per second, regardless of geographical location. The Qwest Team provides information security services to most Government Agencies as well as the financial, information technology, energy, aerospace, health, entertainment, and publishing industries. We are set apart by the personalization and attention we give to each of our customers. We understand that having a lead engineer assigned as a point of contact along with trained, cleared personnel delivering services provides peace of mind.

6.6.1 Technical Approach to Incident Response Management Service Delivery (L.34.1.6.1)

Qwest 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. Qwest resources include world-class information protection laboratories, and world-wide deployment of proprietary, country-approved tools.

6.6.1.1 Approach to Incident Response Management Service Delivery (L.34.1.6.1(a))

[redacted] to capture and track the information required by any Agency.

[redacted]

[redacted]

[redacted]

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

[redacted]

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

Qwest INRS complies with these required standards, including the Federal Information Systems Management Act of 2002 (FISMA), Federal Information Processing Standards 199, Internet Engineering Task Force (IETF)-RFC2350, US- Corporate Emergency Response Team (CERT), and the National Institute of Standards and Technology (SP) 800-61.

[redacted] The system is available any time from any place over the public Internet. Qwest's IRTS system, a secure data repository for an Agency, is available [redacted] This system will aid by recording and tracking reported events. Authorized Agency contacts will have remote access to the IRTS to run reports and as a tool to manage the INRS program.

6.6.1.2 Benefits of Incident Response Management Services Technical Approach (L.34.1.6.1(b))

Qwest's INRS approach offers user Agencies these benefits, as shown in ***Figure 6.6.1-4***.

Figure 6.6.1-4. Features and Benefits of Qwest INRS Approach

Feature	Benefit	[redacted]
Consistent , Fast, and Skilled Response to Incidents	Responding to incidents systematically so that all the appropriate steps are taken	[redacted]
Quick Recovery from Network Events	Smart response to network threats limits data loss and minimizes overall network disruption.	[redacted]
Life Cycle Approach to INRS	Documented knowledgebase of information provides the Agency with a robust experience that is leveraged for future threats.	[redacted]
Strong Legal Remediation	Agency will have sound documentation and recorded evidence in which to use for remediation activities that may require legal attention.	[redacted]
Regulatory Compliance	Besides of the business reasons for an incident response capability, Agencies must comply with applicable laws, regulations, and policies directing a coordinated, effective defense against information security threats	[redacted]
Analysis of the Current Environment	The Agency will benefit from a consistent, predictable, and effective response to threats with Qwest INRS.	[redacted]
Documentation of the Computing Environment	This documentation is utilized to cover regulatory requirements, which suggest an auditor-ready book for review of all systems	[redacted]

Feature	Benefit	[redacted]
Fully Tested Pilot Implementation	Agency will have peace of mind knowing their trusted partner has a rigorously documented and tested SOP on file and is prepared to respond to threats.	[redacted]
Complete Set of Best Practices Knowledgebase to be used for Agency Operational Procedures	Qwest INRS Best Practices in tandem with the Agency's SOPs provide documentation for Agency employees' threat response.	[redacted]

Qwest's INRS technical approach is effective in providing a means to address FISMA, which requires Government Agencies to institute an information security program with the ability to manage and annually reassess risk. Qwest INRS offering supports the Federal Enterprise Architecture (FEA), as noted in ***Figure 6.6.1-5***.

Figure 6.6.1-5. Qwest INRS Meets FEA Requirements

FEA Requirement	Feature and Substantiation
Improve utilization of Government information resources	The Qwest Team will leverage its experience and lessons learned to improve security techniques, such as effective incident response and restoration. This allows Agencies to focus on core missions and service delivery to constituents.
Improve Service Delivery	Successful processes for minimizing incident impact/exposures; specialized tools
Enhance Cost Savings and Cost Avoidance	Qwest's INRS is supported by certified security professionals. Their expertise enables the Agency to comply with regulations regarding notification of incidents that might expose private information. Qwest's INRS limits Agency staff time identifying and responding to sophisticated network events such as viruses, attacks, and other malicious activity.
Maximize Technology Investments	Access to world-class information protection laboratories and their resources.
Increase Cross-Agency and Inter-Government collaboration	Qwest's INRS enables Agency administrators to share threat response information across various departments in order to ensure malicious activity can be controlled and potentially eliminated across the network. A smart, collective effort to thwart expensive intrusions and disruptions is the best collaborative defense.
Simplify Processes and Unify Work across Agencies	The Qwest Team offers worldwide deployment of incident expertise with country-specific tools.
Improve Performance Metrics	Core staff of industry-recognized incident response experts.

6.6.1.3 Solutions to Incident Response Management Services Problems (L.34.1.6.1(c))

During [redacted] operation a variety of problems have arisen and we have instituted effective solutions. We codify the lessons learned and apply them to improve methods. ***Figure 6.6.1-6*** presents several potential problems and our solution/mitigation approach.

Figure 6.6.1-6. Anticipated INRS Problems and Qwest Solutions

Problem	[redacted]
Many users are not incident response experts.	[redacted]
Agencies may have unique networks, systems, architectures, or requirements.	[redacted]
Incidents don't always happen during standard business hours.	[redacted]

6.6.2 Satisfaction of Incident Response Management Services Performance Requirements

6.6.2.1 Incident Response Management Services Quality of Service (L.34.1.6.2(a))

Our Incident Response Service performance metrics are shown in ***Figure 6.6.2-1***.

Figure 6.6.2-1. 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]

Qwest 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 are able to meet each of these performance requirements by staffing our SOC 24x7x365. Qwest has the necessary resources available to respond to incidents encountered by Agencies.

6.6.2.2 Approach for Monitoring and Measuring Incident Response Management Services (L.34.1.6.2(b))

All incident response reports are tracked in our [redacted] Trouble Ticket System. Reports are processed by analysts according to an established work flow and response times are tracked for each report and event.

6.6.2.3 Verification of Incident Response Management Services (L.34.1.6.2(c))

Data to support the measurement of the Government-specified KPIs is collected on a continuous basis; computed statistics are made available to authorized customer personnel [redacted]. The raw data is collected through the INRS system, network, and availability monitoring tools, and through our customer change/problem tracking system.

6.6.2.4 Incident Response Management Services Performance Requirements (L.34.1.6.2(d))

[redacted]

[redacted]

6.6.2.5 Additional Incident Response Management Services Performance Metrics (L.34.1.6.2 3(e))

[redacted]

6.6.3 Satisfaction of Incident Response Management Services Specifications (L.34.1.6.3)

The Qwest Team will provide a time-tested INRS from our 24x7x365 SOC. [redacted]

Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for INRS. The following Figure 6.6.3-1 and Section 6.6.3.1.3 summarize Qwest's response to the INRS capabilities listed in RFP C.2.10.5.1.4, features of RFP C.2.10.5.2, and interfaces of RFP C.2.10.5.3. These subsections are intended to provide the technical description required per L.34.1.6.3(a) and do not limit or caveat Qwest's compliance in any way.

6.6.3.1 Satisfaction of Incident Response Management Service Requirements (L.34.1.6.3(a))

Because of our broad inter-Agency view, we will provide notification of threats to Agencies well in advance, protecting them from incidents in the long run. Examples of this support are as follows:

Fraud/Incident Support: Qwest will provide expert, incident-specific support before, during, and after investigations of 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.

6.6.3.1.1 Satisfaction of INRS Capability Requirements (L.34.1.4.2(a); C.2.10.5.1.4)

Qwest INRS offering meets the required capabilities as shown in ***Figure 6.6.3-1***.

Figure 6.6.3-1. Qwest 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]

Required INRS Capabilities	[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 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	[redacted]

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

6.6.3.1.2 Satisfaction of INRS Interface Requirements (L.34.1.4.2(a); C.2.10.5.3)

All incident response analysis and recommendations will be available [redacted]

6.6.3.2 Proposed Enhancements for Incident Response Management Services (L.34.1.6.3(b))

[redacted]

6.6.3.3 Network Modifications Required for Incident Response Management Services Delivery (L.34.1.6.3(c))

[redacted]

6.6.3.4 Experience with Incident Response Management Services Delivery (L.34.1.6.3(d))

Qwest has many years of experience in providing INRS for large and small organizations and Government Agencies with multiple platforms and products. [redacted]

[redacted]

[redacted]

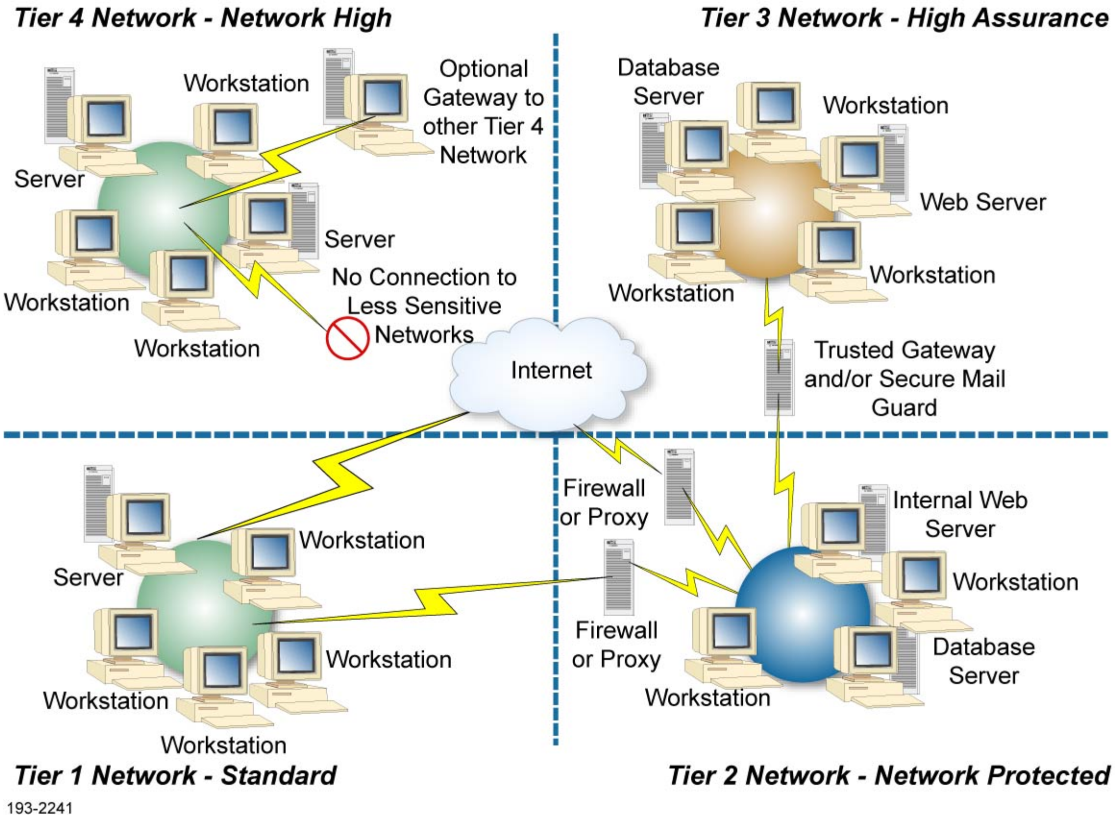
Our INRS monitors the US-CERT and was asked for assistance with Presidential Decision Directive 63 (PDD-63). PDD-63 focused on securing the nation’s critical infrastructures, and as a trusted advisor in this area, we helped establish and support the first Financial Services ISAC (FS/ISAC).

6.6.3.5 Managed Tiered Security Services (MTSS) Approach (L.34.1.6.3(e))

INRS is part of Qwest's MTSS technical solution. Design, implementation and delivery according to GSA's MTSP, ***Figure 6.6.3-2***, will be addressed to meet an Agency’s requirements based on security service levels identified as described in Section 6.8. A defense-in-depth strategy and technical solution that includes INRS best practices will be structured to the network architecture as described in 6.8.3.1.1.

MTSP Tier 2 - Protected Service will provide security enhancements to the subscribing Agency with additional protection from unauthorized activities and the proliferation of malicious code. Protected service will also mitigate the potential for Denial of Service attacks. Security enhancements include a

Figure 6.6.3-2. MTSP Notional Architecture



combination of firewall, premises-based virtual private network (encrypted tunnels), filtering router, proxy server, and boundary anti-virus detection technologies configurable to the subscribing Agency's security policy(s) and specifications.

Tier 2 is tailored to Sensitive But Unclassified mission functions and information. It employs both technical and network management components appropriate to the respective mission and/or information sensitivity.

[redacted]