Security

Services Provided

Network Security

Services provided include intrusion prevention and detection (IPS/IDS), vulnerability scanning and remediation, audit logging/monitoring and security patch management.

Security Incident Management

Incident management and forensic collection and analysis are provided for reporting and remediation of security issues.

Data Security

Services provided include encryption, media sanitization, malicious code protection and application security support.

Security Program Management

ITS provides certification and Accreditation (C&A) support for the client agency C&A process, including Security Testing and Evaluation (ST&E) efforts, and providing network, scanning, and hosting support during evaluations.

Continuity Services

This service offer covers all requirements for contingency planning as specified under the Homeland Security requirements as administered by FEMA. This service covers support for both Continuity of Operations Planning (COOP) and Disaster Response Testing/Recovery.

Personnel Security

This service provides security training, awareness, and completion of security agreements.

Performance Matrix & Targets

Reporting is subject to baseline measurements and vendor limitations.

Security			
Service Type	**Service Measure**	**Measurement**	**Performance Target**
Security Incident reportable to USDA/OCIO/ASOC	Notification Time	Customer Alert <30 minutes after discovery or within Cyber Security guidelines ITS Logs	95%
Incident Handling	Respond and Assess	< 4 hours ITS Response Time – USDA/OCIO/ASOC Incident Notification Time ITS Logs	99%
Incident Research	Review and Provide assessment	< 3 business days ITS Logs	99%
Incident Resolution	Duration of Incident Resolution	OCIO/CS Timeline Requirement (varies per incident type) Incident Resolution Time – OCIO/CS Incident Notification Time ITS Logs	99%
Network Scanning	Completion of Task	Quarterly Months in FISMA compliance ÷ 12 (Rolling Average) ITS Scan Database Reports Scanning is limited to systems connected directly to the ITS network environment.	98%
Vulnerability Remediation	Vulnerability Assessment	Vulnerabilities identified from scans each month are reviewed and appropriate actions initiated. • Remediate, • Validate False Positive, • Initiate Acceptance Paperwork • ITS Scan Database Reports	90%