1.1.3 Business Support Systems [G.5]

We propose our [redacted] system, the MetTel EIS Portal, for our Business Support Systems (BSS) to support efficient and effective management of EIS services. We leverage our experience with the Government and commercial customers to provide an intuitive and fully functional BSS. We simply merged the Government-unique and individual Task Order requirements into our comprehensive MetTel EIS Portal to provide a [redacted] for working with all aspects of our infrastructure systems, eliminating the need for MetTel to [redacted]

Unparalleled Web Portal

- All MetTel Service Management-related activities are available online 24×7×365
- [redacted]
- [redacted]
- Modules for pricing, ordering, billing, customer support, inventory, [redacted] management

Shown in **Exhibit 1.1.3-1**, the MetTel EIS Portal assists users with pricing, ordering, billing, customer support, inventory, [redacted] in an automated, easy-to-use, graphically based online system available 24×7×365. The MetTel EIS Portal is an enhanced and secure network infrastructure with a common centralized database platform and electronic information exchange capabilities such as Electronic Data Interchange (EDI).

[redacted]

Exhibit 1.1.3-1. MetTel EIS Portal Dashboard

The MetTel EIS Portal comprises a [redacted] Dashboard that serves as a landing page for users to view orders, [redacted] as well as the Billing, Services, [redacted] and Ordering modules. Each of these modules are described and shown below.

[redacted]

Exhibit 1.1.3-2. Billing Module Percentages Spent

Exhibits 1.1.3-2 and **1.1.3-3**, the **Billing Module** is used to search and view charge history and account details, add accounts, and upload and download invoices.

[redacted]

Exhibit 1.1.3-3. Billing Module Order Status

Shown in **Exhibit 1.1.3-4**, the **Services Module** is used to view inventory and locations of service by geography, organization, or billing account.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Exhibit 1.1.3-4. Services Module List View

Exhibit 1.1.3-5 shows a sample of pending installations and repair and services by location, graphed by cost per month. The graph displays a timeline representing the number of tickets opened each day.

[redacted]

Exhibit 1.1.3-5. Services Module Graphical View

Shown in **Exhibit 1.1.3-6**, the **Reports Module** is used to set up recurring reports, [redacted] and view historical reports. [redacted] use the dropdown filter to select from a variety of categories. Reports are viewable only by users with role-based permissions (e.g., users assigned to a billing role have access to Billing Reports). [redacted]

[redacted]

Exhibit 1.1.3-6. Reports Module

Exhibit 1.1.3-7 lists the report categories already available in the MetTel EIS Portal and report types for each.

Exhibit 1.1.3-7. Report Types

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

Shown in **Exhibit 1.1.3-8**, the **Help Desk Module** is used for entering new services, canceling existing services, [redacted]. The MetTel EIS Portal displays

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

ticket data including the Age of the Ticket, Ticket Type, Number, and Status.

[redacted]

Exhibit 1.1.3-8. Help Desk Module

The primary page displays all tickets associated with a user. All Government tickets are displayed by location of the service [redacted]

Users sort tickets by Status Age (the default), Type including the person who last viewed the ticket and the Ticket Number.

Shown in **Exhibit 1.1.3-10**, the **Ordering Module** is used to shop for new devices and telecommunications services at contracted rates. Customers may shop for pre-approved devices and services through the MetTel EIS Portal catalog, [redacted]

[redacted]

[redacted]

Exhibit 1.1.3-10. Ordering Module

Customer Usage. MetTel provides customers with a powerful and extremely comprehensive Portal, the MetTel EIS Portal, enabling MetTel customers to manage their inventory, usage, billing, service, [redacted] more from one simple, user-friendly interface. [redacted]

[redacted]

[redacted]

Our CSRs facilitate the MetTel EIS Portal training. They then solicit and record client feedback in real time. We also request survey feedback at the end of each course and collect user requirements from daily use of the Portal. We forward all feedback to product marketing for possible upgrades to the MetTel EIS Portal.

1.1.3.1 Overview [G.5.1]

We fully understand the requirement for the BSS and provide the MetTel EIS Portal to satisfy the requirements for a single integrated system, described above.

1.1.3.2 Satisfaction of Technical Requirements [G.5.3]

1.1.3.2.1 Web Interface [G.5.3.1]

The MetTel EIS Portal is our BSS web interface and adheres to common industry standards. The Portal does not require special software or plug-ins beyond standard web browsers with default built-in functionality and already supports these products:

- Microsoft Internet Explorer/Microsoft Edge (desktop and mobile)
- Google Chrome (desktop and mobile)
- Mozilla Firefox (desktop and mobile)
- Apple Safari (desktop and mobile)

We are committed to supporting these browsers in their current and two previous versions (N-2) and will continuously update them to support any successor versions.

MetTel EIS Portal fully complies with 508 Accessibility standards [redacted] and also supports all required functionality.

Within 30 days of a Notice To Proceed (NTP), we provide on our website a comprehensive list of all offered Electronic and Information Technology (EIT) products that fully comply with Section 508 of the Rehabilitation Act of 1973, as amended, and with the Architectural and Transportation Barriers Compliance Board's Electronic and IT Accessibility Standards 36 CFR Part 1194.

We completed a Voluntary Product Accessibility Template (VPAT) for the MetTel EIS Portal which is available on our website. The VPAT directly addresses compliance with Section 508 in the following deliverables: BSS Development and Implementation

Plan, BSS Verification Test Plan and BSS Verification Test Results. We performed the three-step process shown **in Exhibit 1.1.3-11** to ensure full compliance.

Exhibit 1.1.3-11. Compliance Process

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

1.1.3.2.2 Direct Data Exchange [G.5.3.2]

The MetTel EIS Portal includes secure, automated mechanisms for direct transfer of detailed transaction data to the GSA Conexus. This data covers all elements detailed in Section G.5.4 BSS Component Service Requirements.

Our BSS initiates and processes bi-directional automated exchange of management and operations data using:

Web Services: Transactions over HTTPS via our Business to Business (B2B) APIs for system-to-system data exchange between Government and contractor systems. We support XML over HTTPS using Simple Object Access Protocol (SOAP) as the web services exchange mechanism. The transactions are bi-directional.

GSA Conexus System: Support of the GSA Conexus system utilizing X.509-based digital certificates to support mutual authentication and encryption as well as HTTPS as the protocol for secure web services between MetTel systems and GSA Conexus. We observe the NIST SP 800-95 Guide to Secure Web Services as well as other references identified in NIST SP 800-53 R4 and GSA Web Application Security Guide 07-35.

Secure File Transport Protocol (SFTP) Services: Transactions for file-based data exchange between Government and MetTel systems using Government-provided FTP service. Transactions include transfer of data from the Government to MetTel and from MetTel to the Government.

Our BSS accepts data transfers from the Government and submits data to the Government in the formats specified in Section J.2.9. We acknowledge that GSA has the right to maintain and manage all approved data exchange format specifications, data schemas, and method descriptions. We further understand that once the BSS is in operation, we may not make any changes to the data exchange formats or methods without Government approval via the established change control process defined in Section G.5.5.1 BSS Change Control.

1.1.3.2.3 Role Based Access Control [G.5.3.3]

We collect user registration and Role Based Access Control (RBAC) information from the Government customer to set up access control on the MetTel EIS Portal as described Section J.2.3.

1.1.3.2.4 Data Detail Level [G.5.3.4]

We fully understand that all data to be provided by the BSS must be sufficiently detailed to provide all data elements relating to the services listed in Section G.5.4. BSS deliverables are provided in human- and machine-readable formats as requested.

1.1.3.3 Satisfaction of BSS Component Service Requirements [G.5.4]

Exhibit 1.1.3-12 shows the functionality we provide in the MetTel EIS Portal.

Exhibit 1.1.3-12. The MetTel EIS Portal Services and Functionality

Service	Minimum Functionality	[redacted]
Customer Management	a) User Training b) [redacted]	[redacted]
Financial Management	c) Billing Management d) Payment Tracking e) Disputes f) [redacted]	[redacted]
Order Management	g) Order Submission h) Order Tracking	[redacted]
Inventory Management	i) Inventory Management	[redacted]
Service Management	j) Service Assurance k) [redacted]	[redacted]
Program Management	l) Administration m) Project Management n) Reporting o) Service Catalog	[redacted]

1.1.3.4 BSS Development [G.5.5; F.2.1(39)]

We document specific details of the development process and approach in the MetTel Federal BSS Development and Implementation Plan included in Section 1.1.3.7.

We fully acknowledge that we are solely responsible for all development, testing, and maintenance including but not limited to security validation functional testing and configuration control. Additionally, we provide upgrades to our BSS at no additional cost to the Government as upgrades become available. We acknowledge the BSS functional testing requirements defined in E.2.1 and BSS security testing requirements in G.5.6.

1.1.3.4.1 BSS Change Control [G.5.5.1; F.2.1(40)]

The MetTel change control process is already fully developed and documented. Any changes to the BSS that fall under one or more of these five categories are under change control: web interface that impacts Section 508 compliance, required Government personnel training, impacts to the Direct Data Exchange (Section G.5.3.2.1), impacts to the ability of BSS to meet any specified requirements, and impacts to system security. We notify the Government at least 30 days prior to BSS changes requiring change control. Further, we agree to:

1. Obtain Government approval before implementing a change
2. Use industry-standard change control procedures
3. Train Government personnel if required
4. Retest with the Government to ensure functionality continues to meet requirements
5. Update all relevant service documents and information posted on our website(s) as necessary within 7 days of completing the change and at no additional cost to the Government

For changes that meet the standards of eligibility for change control, we follow industry-standard change control procedures and conditions. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

All procedures are at no additional cost to the Government. We schedule and deliver any additional training tailored to Government requirements.

1.1.3.5 BSS Security Requirements [G.5.6]

All security requirements are met for the MetTel EIS Portal as defined in our BSS System Security Plan (SSP) and:

- Our BSS SSP is based on the NIST FIPS-199 labeling of Moderate Impact.
- We have selected the appropriate controls for Moderate Impact system from each of the Control Families as specified in NIST SP 900-53 Rev.4.
- We support the Government's efforts to verify that these standards are met.

1.1.3.5.1 Satisfaction of General Security Compliance Requirements [G.5.6.1]

We understand that we are subject to all current applicable and Federal Agency-specific IT security directives, standards, policies, and reporting requirements, and we comply with the Federal Information Security Management Act (FISMA) guidance and directives to include: Federal Information Processing Standards (FIPS), NIST Special

Publication (SP) 800 series guidelines, GSA IT security directives, policies, and guides, and other appropriate Government-wide laws and regulations for the protection and security of Government IT.

1.1.3.5.2 GSA Security Compliance Requirements [G.5.6.2]

Based on the criteria specified in FIPS-199 and FIPS-200, our BSS is categorized at the Moderate Impact level. We also submit a Risk Management Framework Plan (Attachment 7) that describes our approach for BSS security compliance at the Moderate Impact level as well as our Risk Management Framework Plan in accordance with NIST SP 800-37.

1.1.3.5.3 Security Assessment and Authorization [G.5.6.3]

Our BSS has a valid Security Assessment and Authorization (A&A) prior to processing Government information. Additionally, we acknowledge and fully understand:

- Our failure to maintain a valid security A&A is grounds for contract termination.
- We will conduct a new security A&A on our BSS at least every 3 years or when a significant change impacts the system security posture.

1.1.3.5.4 BSS System Security Plan [G.5.6.4]

We comply with all security A&A requirements as mandated by federal laws, directives, and policies, including making available any documentation and physical and logical access needed to support this requirement. The level of security A&A is based on the system’s NIST FIPS- 199 categorization of Moderate Impact.

Our BSS SSP is in accordance with NIST SP 800-18, and the BSS SSP is completed and submitted within 30 days of the NTP to include annual updates. We create, maintain, and update the security A&A documentation listed in **Exhibit 1.1.3-14**.

Exhibit 1.1.3-14. Security A&A Documentation List

Item #	Documentation	Description
1.	(BSD	Develop/maintain aSecurity Assessment Boundary & Scope Document (BSD) as identified in NIST SP 800-18, & we complete and submit our within 15 days of NTP, updated annually.
2.	ISA	We develop & maintain Interconnection Security Agreements (ISAs) in accordance with NIST SP 800-47 and provide any ISAs with the initial security A&A package updated annually.
3.	GSA NIST SP 800-53 R4 Control Tailoring Workbook	We develop and maintain a GSA Control Tailoring Workbook as identified in GSA Security Procedural Guide 06-30 Managing Enterprise Risk. We document all MetTel-implemented settings that are different from the GSA settings and provide a Control Tailoring Workbook for

Item #	Documentation	Description
		the MetTel BSS with the initial security A&A package to include annual updates.
4.	GSA Control Summary Table for a Moderate Impact Baseline	We develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30 Managing Enterprise Risk. We provide a GSA NIST SP 800-53 R4 Control Summary Table for our BSS with the initial security A&A package to include annual updates.
5.	Rules of Behavior (RoB)	We develop and maintain an RoB for our BSS users as identified in GSA IT Security Procedural Guide 06-30 Managing Enterprise Risk and Order CIO 2104.1 IT General RoB. We provide an RoB for our BSS with the initial security A&A package updated annually.
6.	System Inventory	We develop and maintain a System Inventory that includes hardware, software, and related information as identified in IT Security Procedural Guide 06-30 Managing Enterprise Risk. We provide a System Inventory for our BSS w/ the initial security A&A package updated annually.
7.	Contingency Plan (CP) and BIA	We develop and maintain a CP including a Disaster Recovery Plan (DRP) & Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34. We provide a CP, DRP, and BIA for our BSS with the initial security A&A package to include annual updates.
8.	Contingency Plan Test Plan (CPTP)	We develop and maintain a CPTP completed in agreement with GSA IT Security Procedural Guide 06-29 Contingency Planning Guide. We provide a CPTP for our BSS with the initial security A&A package to include annual updates.
9.	Contingency Plan Test Report (CPTR)	We test the CP and document the results in a CPTR, in agreement with GSA IT Security Procedural Guide 06-29 Contingency Planning Guide. We provide a CPTR for our BSS with the initial security A&A package to include annual updates.
10.	Privacy Impact Assessment (PIA)	We perform a PIA per GSA IT Security Procedural Guide 06-30 Managing Enterprise Risk. We provide a PIA for our BSS with the initial security A&A package updated annually.
11.	Configuration Management Plan	We develop and maintain a Configuration Management Plan (CMP) and provide a CMP for our BSS with the initial security A&A package to include annual updates.
12.	System(s) Baseline Configuration Standard Document	We develop and maintain a System(s) Baseline Configuration Standard Document and a well-defined, documented, and up-to-date specification to which our BSS is built. We provide the System Baseline Configuration for our BSS as a part of the CMP and submit it with the initial security A&A package to include annual updates.
13.	System Configuration Settings	We develop and maintain System Configuration Settings and establish and document mandatory configuration settings for IT products employed within our BSS that reflect the most restrictive mode consistent with BSS operational requirements. Our BSS is configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practices in hardening systems, as deemed appropriate by the Administrative Officer (AO). Our BSS configuration settings are included as part of the CMP, which we update and/or review on an annual basis.
14.	Incident Response Plan (IRP)	We develop and maintain an IRP and provide an IRP for our BSS with the initial security A&A package to include annual updates.
15.	Incident Response Test Report (IRTR)	We test the IRP and document the results in an IRTR and provide an IRTR for our BSS with the initial security A&A package to include annual updates.
16.	Maintenance of System Security	We develop and maintain a Continuous Monitoring Plan to document how monitoring of our BSS is accomplished. Continuous monitoring, security controls, and supporting deliverables are updated and submitted to GSA per a mandated schedule. We provide a Continuous Monitoring Plan for our BSS with the initial security A&A package to include annual updates.

Item #	Documentation	Description
17.	Plan of Action and Milestones (POA&M)	We develop and maintain a POA&M completed in agreement with GSA IT Security Procedural Guide 06-30 Plan of Action and Milestones. All scans associated with the POA&M are performed as an authenticated user with elevated privileges. Vulnerability scanning results are managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. All scans include all networking components that fall within the BSS security accreditation boundary. The appropriate vulnerability scans are also submitted with the initial security A&A package, and an annual BSS User Certification/Authorization Review is annotated on the POA&M. We provide a POA&M for our BSS as part of the initial security A&A package followed by quarterly updates.
18.	Independent Penetration Test Report	FIPS-199 Moderate Impact systems complete an independent internal and external penetration test and provide a report documenting the results of the vulnerability analysis and exploitability of identified vulnerabilities with the security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA provides for the scheduling and performance of these penetration tests, and all penetration test exercises are coordinated through the GSA Office of the Chief Information Security Officer (OCISO) Security Engineering division at itsecurity@gsa.gov per GSA CIO-IT Security Guide 11-51.
19.	Code Review Report	All FIPS 199 Moderate Impact systems conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools to examine for common flaws. We document those results in a Code Review Report that we submit prior to placing our BSS into production when there are changes to code and also on an annual basis. If applicable, a Code Review Report is submitted as an initial deliverable prior to placing our BSS into production, on an annual basis and when there are changes to code.
20.	Security/Risk Assessment Report (SAR)	We allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities to include control reviews per NIST SP 800-53 R4 / NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30 Managing Enterprise Risk. Review activities include but are not limited to OS vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Government information. This includes the BSS infrastructure, and all scans are performed as an authenticated user with elevated privileges.
21.	POA&M document	We track all identified gaps between the required 800-53 R4 controls and BSS implementation as documented in the SAR for mitigation in a POA&M document that we complete in accordance with GSA IT Security Procedural Guide 09-44, POA&M.
22.	Mitigating Risks	We mitigate continuous monitoring activities and all security risks found during the security A&A. All critical and high-risk vulnerabilities are mitigated within 30 days, and all moderate risk vulnerabilities are mitigated within 90 days from the date vulnerabilities are formally identified. GSA determines the rating of vulnerabilities, and monthly updates are provided on the status of all critical and high vulnerabilities that have not been closed within 30 days.
23.	Annual FISMA Assessment	We deliver the results of our annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26 FISMA Implementation. Our annual assessment is completed each fiscal year in accordance with instructions provided by GSA.
24.	Policy and Procedure Documents	We develop and maintain all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides. The list of documents in § G.5.6.4 – 24 is verified and reviewed during the initial security assessment, and updates are provided to the GSA COR/ISSO/ISSM biennially.

1.1.3.5.5 Additional Security Requirements [G.5.6.6]

We adhere to proper privacy and security safeguards in accordance with FAR Part 52.239-1. Deliverables identified in Section G.5.6.4 are labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) and/or with a MetTel designation per document sensitivity. We acknowledge that external transmission/dissemination of CUI data to or from a GSA computer must be encrypted. Certified encryption modules must be encrypted and used in accordance with FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Where appropriate, we ensure implementation of the requirements identified in FAR 52.224-1 Privacy Act Notification and FAR 52.224-2 Privacy Act.

We cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal Government's agent.

We understand that the Government has the right to perform manual and/or automated audits, scans, reviews, or other inspections of our BSS IT environment used to provide and/or facilitate services in accordance with the FAR.

1. We do not publish and/or disclose in any manner, without the CO's written approval, the details of any safeguards designed and/or developed by MetTel under the EIS contract or otherwise provided to the Government, except for disclosure to a consumer Agency for the purposes of A&A verification.

2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the contractor, we provide the Government logical and physical access to our facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of request. Automated audits include but are not limited to the following methods:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Internal and external penetration testing

3. Government personnel or agents acting on behalf of the Government can automate scans using Government-operated equipment and Government-specified

tools. We provide all MetTel-initiated scans and results to the Government. We understand that if we perform our own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government-performed vulnerability scans. Our scanning tools and configurations require Government approval.

We perform personnel security/suitability in accordance with FAR Part 52.204-9. All MetTel contractor personnel with access to Government information within the security A&A scope successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11, and as specified in GSA CIO Order 2100.1J and GSA Directive 9732.1D Suitability and Personnel Security. The Government is responsible for the cost of such background investigations.

1.1.3.6 Data Retention [G.5.7]

We fully understand and comply with the data retention requirements of FAR Subpart 4.7 (48 CFR 4.7) and agree to maintain and archive all records for 3 years after final payment under the contract.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]