



MISSION REQUIREMENTS SURVEY

Tell us the mission need.

Use this survey to give FEDFORTRESS enough context to understand the problem, identify the disciplines involved, and prepare a practical next step. Complete only the sections relevant to your request. "Unknown" is an acceptable answer.

IMPORTANT - PUBLIC INTAKE TEMPLATE

Do not enter classified information, CUI, FCI, export-controlled technical data, credentials, personally sensitive information, or sensitive program details. If protected information is needed for discovery, contact FEDFORTRESS first to coordinate an approved transfer method.

01 Project and point of contact

Organization / Company

Project / Program

Primary POC

Title / Role

Date

Email

Phone

02 What type of support are you seeking?

☐ Cybersecurity / RMF / ATO

☐ IT infrastructure / modernization

☐ Network engineering / integration

☐ Cloud / Microsoft 365 / GCC High

☐ Physical security / secure facilities

☐ Custom application / software development

☐ System hardening / STIG / ACAS

☐ CMMC / NIST compliance support

☐ Equipment procurement / integration

☐ Engineering / technical advisory

☐ Other

☐ Not sure - help us determine the approach

If other, briefly describe

03 Mission need and desired outcome

What problem are you trying to solve, and what is not working today?

What would a successful outcome look like?

Continue only with the sections that apply to your request. Skip anything that is not relevant or not yet known.



ENGAGEMENT, SCHEDULE & PERFORMANCE

04 Engagement context

- ☐ U.S. Government organization
- ☐ Prime contractor
- ☐ Commercial organization

- ☐ State / local government
- ☐ Subcontractor / teammate
- ☐ Other / not yet determined

Technical POC**Contracting / Business POC****Prime / Customer, if applicable****Contract / Solicitation No., if known****Current request / acquisition stage**

- | | |
|---|---|
| ☐ Early discovery / requirements | ☐ Site survey / assessment |
| ☐ ROM / budgetary estimate | ☐ Formal proposal / quote |
| ☐ Implementation / integration | ☐ Remediation / recovery |
| ☐ Operations / sustainment | ☐ Unknown / need guidance |

05 Schedule and place of performance

Desired response / proposal date**Desired start date****Desired completion / IOC****Primary place of performance****Number of sites / locations****Approx. users****Known schedule drivers, outages, access windows, dependencies, or milestones**

06 Mission criticality and support expectations

- | | |
|---|--|
| ☐ Mission-critical operation | ☐ Downtime / outage sensitive |
| ☐ After-hours work may be required | ☐ On-site support expected |
| ☐ Remote support acceptable | ☐ Support model not yet defined |

Operating hours, response expectations, maintenance windows, staffing, or sustainment needs



INFORMATION SENSITIVITY & OPERATING ENVIRONMENT

07 Information / data sensitivity

Indicate categories only. Do not include classified program names, protected technical details, or other sensitive specifics in this public intake form.

- | | |
|---|---|
| ☐ Public / non-sensitive | ☐ Unclassified |
| ☐ FCI | ☐ CUI |
| ☐ Secret | ☐ Top Secret |
| ☐ SCI | ☐ SAP / special access |
| ☐ Other | ☐ Unknown / to be determined |

Non-sensitive notes about handling, marking, transmission, or data ownership requirements

08 Network / operating environment

- | | |
|---|---|
| ☐ Commercial Internet / enterprise LAN | ☐ Standalone / air-gapped |
| ☐ NIPRNet | ☐ SIPRNet |
| ☐ JWICS | ☐ DREN |
| ☐ CANES / platform environment | ☐ Other Government enclave |
| ☐ Cloud-hosted | ☐ Hybrid on-prem / cloud |
| ☐ Lab / test environment | ☐ Unknown / to be determined |

Boundary, hosting, enclave, connection, or deployment context

09 External connections and dependencies

- | | |
|--|---|
| ☐ Internet access required | ☐ Cross-domain or data-transfer dependency |
| ☐ Partner / contractor network dependency | ☐ Cloud service dependency |
| ☐ Remote administration / access required | ☐ No external connection expected |
| ☐ Unknown / not yet defined | |

External systems, services, organizations, data exchanges, or approvals that may affect the solution



IT INFRASTRUCTURE & MODERNIZATION

10 Current environment snapshot

Approx. endpoints	Physical servers	Virtual machines	Network devices
Primary directory / identity	Primary client OS	Primary server OS	
Virtualization / hypervisor	Cloud environment	Email / collaboration	
Key existing platforms, vendors, hardware, software, and major constraints			

11 Infrastructure scope

- | | |
|---|---|
| ☐ Workstations / laptops | ☐ Servers / virtualization |
| ☐ SAN / NAS / storage | ☐ Backup / recovery |
| ☐ Switching / routing | ☐ Firewall / perimeter |
| ☐ Wireless | ☐ Remote access / VPN |
| ☐ Identity / access management | ☐ Microsoft 365 / GCC High |
| ☐ Azure / Azure Government | ☐ AWS / AWS GovCloud |
| ☐ Logging / SIEM | ☐ Monitoring / management |
| ☐ VDI / remote desktop | ☐ Other |

12 Network and connectivity

Internet / WAN bandwidth, if known	Primary firewall / router platform	Primary switching platform
☐ Network segmentation / VLAN changes	☐ Routing changes	
☐ Firewall / ACL changes	☐ DNS / DHCP services	
☐ Wireless design / hardening	☐ VPN / remote access	
☐ QoS / latency requirements	☐ Network requirements not yet defined	
Network topology, ports / protocols, connectivity, throughput, or remote-access requirements		



CAPACITY, RESILIENCE & PROCUREMENT

13 Capacity, availability, and recovery

Estimated storage required

Expected data growth

RPO, if known

RTO, if known

☐ High availability required☐ Backup / restore required☐ Offline / disconnected operation required☐ Hardware / path redundancy required☐ Disaster recovery / alternate site required☐ Availability targets not yet defined**Performance, bandwidth, latency, compute, GPU, storage, retention, concurrency, or recovery requirements**

14 Operations, management, and lifecycle

☐ Central monitoring / alerting☐ Endpoint management / MDM☐ Backup management☐ Out-of-band management☐ Patch / update management☐ Central logging / SIEM☐ Asset / inventory management☐ Post-deployment sustainment required**Operational ownership, maintenance model, lifecycle, warranty, support, or handoff expectations**

15 Procurement and integration constraints

☐ New hardware expected☐ Government-furnished equipment involved☐ Approved-product / vendor restrictions apply☐ Long-lead equipment may affect schedule☐ New software / licensing expected☐ Contractor-furnished equipment expected☐ Reuse existing equipment where practical☐ Procurement path not yet defined**Approved products, vendor preferences, lifecycle limits, licensing, rack / power / cooling, environmental, or integration constraints**



CYBERSECURITY & AUTHORIZATION

16 Cybersecurity support needed

- | | |
|--|--|
| ☐ RMF / authorization support | ☐ ATO / reauthorization support |
| ☐ STIG / SRG hardening | ☐ ACAS / vulnerability scanning |
| ☐ POA&M remediation / closure | ☐ Security architecture / boundary definition |
| ☐ CMMC / NIST 800-171 | ☐ Control evidence / artifact development |
| ☐ Readiness / pre-assessment | ☐ Continuous monitoring / sustainment |
| ☐ Technical procedures / SOPs | ☐ Other cybersecurity support |

17 Authorization state

System / package name (non-sensitive only)

eMASS package established?

Current ATO expiration, if applicable

Current RMF step, if known

- | | | | |
|----------------------------------|-------------------------------------|----------------------------------|------------------------------------|
| ☐ Prepare | ☐ Categorize | ☐ Select | ☐ Implement |
| ☐ Assess | ☐ Authorize | ☐ Monitor | ☐ Unknown |

Desired authorization / assessment outcome

- | | |
|--|--|
| ☐ New ATO | ☐ Reauthorization |
| ☐ IATT | ☐ Assess Only |
| ☐ Reciprocity / inheritance support | ☐ Remediation / POA&M closure |
| ☐ Need guidance | |

Target authorization / assessment date

Authorizing organization / AO, if known

18 Authorization boundary and control implementation

- | | |
|--|---|
| ☐ Authorization boundary already defined | ☐ New boundary must be developed |
| ☐ Control inheritance expected | ☐ Cloud shared-responsibility / inheritance involved |
| ☐ PPSM / ports-protocols-services requirement | ☐ Cross-domain / transfer solution involved |
| ☐ Mobile / removable-media considerations | ☐ Boundary / control model not yet defined |

Known boundary questions, control ownership issues, system interconnections, authorization dependencies, or decision points

FEDFORTRESS can support authorization readiness, engineering, evidence development, assessment preparation, and sustainment. Authorization and risk-acceptance decisions remain with the applicable Government authorizing official.



CYBERSECURITY EVIDENCE & COMPLIANCE

19 Existing artifacts and technical evidence

- | | |
|---|---|
| ☐ System Security Plan / security plan | ☐ Hardware inventory |
| ☐ Software inventory / SBOM | ☐ Network / data flow diagrams |
| ☐ STIG / SRG checklists | ☐ ACAS / Nessus scan results |
| ☐ POA&M | ☐ Risk / assessment report |
| ☐ Control implementation statements | ☐ PPSM / port-protocol data |
| ☐ Prior authorization package / decision | ☐ Limited or no existing package |

20 Frameworks and technical baselines

- | | |
|--|---|
| ☐ NIST SP 800-53 / RMF controls | ☐ NIST SP 800-171 / CMMC |
| ☐ DISA STIG / SRG | ☐ FIPS-validated cryptography requirements |
| ☐ FedRAMP / cloud control inheritance | ☐ Customer-specific security baseline |
| ☐ Privacy / PII requirements | ☐ Other framework or mandate |

21 Tools, scans, and access

- | | |
|---|---|
| ☐ eMASS access / exports | ☐ ACAS / Tenable |
| ☐ STIG Viewer / Viewer data | ☐ Evaluate-STIG / automation |
| ☐ EDR / Defender / endpoint security | ☐ SIEM / centralized logging |
| ☐ MDM / endpoint management | ☐ Other vulnerability / compliance scanner |

Available tools, credentials/access process, scan windows, repositories, or evidence sources

22 Known findings and compliance priorities

Known findings, control gaps, recurring vulnerabilities, POA&M priorities, audit issues, or compliance deadlines

What cybersecurity outcome would make this engagement successful?



PHYSICAL SECURITY & SECURE FACILITIES

23 Physical security scope

- | | |
|--|--|
| ☐ Physical security site survey | ☐ Secure room / secure facility support |
| ☐ SCIF support / coordination | ☐ SAPF support / coordination |
| ☐ Access control / badging | ☐ Intrusion detection / alarms |
| ☐ CCTV / video management | ☐ Visitor management |
| ☐ Secure storage / containers | ☐ Locks / doors / barriers |
| ☐ Security drawings / documentation | ☐ Physical / cyber system integration |

24 Facility profile

Facility / site name (non-sensitive only)

City / State / general location

Approx. rooms / spaces

- | | | |
|---|---|--|
| ☐ Existing facility | ☐ New facility / new space | ☐ Renovation / modification |
| ☐ Temporary / deployable | ☐ Shipboard / platform | ☐ Not yet determined |
| ☐ Office / admin space | ☐ Lab / engineering space | ☐ Server / network room |
| ☐ Operations area | ☐ Classified secure space | ☐ Other |

25 Existing systems and documentation

- | | | |
|---|---|---|
| ☐ Access control system | ☐ Intrusion detection system | ☐ CCTV / VMS |
| ☐ Alarm monitoring | ☐ Visitor / badging system | ☐ Secure storage |
| ☐ UPS / emergency power | ☐ No existing system / greenfield | ☐ Unknown |
| ☐ Floor plans / as-builts | ☐ Security / low-voltage drawings | |
| ☐ Existing equipment inventory | ☐ Prior accreditation / approval artifacts | |
| ☐ Site photos (non-sensitive) | ☐ Customer security requirements / standards | |

26 Site constraints and desired result

Site access / escort limitations

Target inspection / acceptance / accreditation date

- | | |
|--|---|
| ☐ Construction / renovation involved | ☐ After-hours work may be required |
| ☐ Work in occupied / operational space | ☐ New low-voltage cabling expected |
| ☐ Government approval / inspection required | ☐ Constraints not yet known |

Describe the physical security problem, desired end state, and any known facility constraints



CUSTOM APPLICATIONS & SOFTWARE

27 Application profile

- | | | | |
|--|---|--|--|
| ☐ Web application | ☐ Desktop application | ☐ Mobile application | ☐ API / service |
| ☐ Automation / workflow tool | ☐ Data / analytics application | ☐ System integration / middleware | ☐ Other |
| ☐ Concept / requirements only | ☐ New development | ☐ Prototype / MVP | |
| ☐ Enhancement to existing application | ☐ Modernization / migration | ☐ Sustainment / defect correction | |

Application / project name**Estimated users****Concurrent users****Target platform(s)**

--	--	--	--

28 Hosting, identity, and integration

- | | | |
|--|--|---|
| ☐ On-premises | ☐ Government cloud | ☐ Commercial cloud |
| ☐ Air-gapped / disconnected | ☐ Hybrid | ☐ Not yet determined |
| ☐ CAC / PIV | ☐ Entra ID / Azure AD | ☐ Active Directory |
| ☐ Federated SSO | ☐ Local accounts | ☐ Service / API accounts |
| ☐ Unknown | | |

Required interfaces, APIs, databases, file exchanges, devices, or external systems

--

29 Security and engineering requirements

- | | | |
|--|--|--|
| ☐ Role-based access control | ☐ Audit logging / traceability | ☐ Encryption in transit / at rest |
| ☐ Offline operation | ☐ SBOM / dependency inventory | ☐ STIG / SRG hardening |
| ☐ Section 508 accessibility | ☐ CI/CD / DevSecOps | ☐ Containerized deployment |
| ☐ Reporting / export | ☐ MDM / managed mobile deployment | ☐ RMF / ATO support required |

30 Existing codebase, schedule, and core workflow

Existing language / framework**Repository / version control**

--	--

Target MVP / prototype date**Target production date****Customer source ownership required?**

--	--	--

Describe the workflow, user problem, core features, and what the application must enable

--



ACQUISITION, DELIVERABLES & CUSTOMER INPUTS

31 Acquisition and contracting context

Contract vehicle / channel, if known

Solicitation / task order / RFQ number

Response due

☐ Planning / unfunded requirement☐ Funding pending☐ Funded / ready to execute☐ Phased funding expected☐ Unknown / not provided☐ Remote☐ On-site☐ Hybrid☐ Travel expected☐ Escort / special access required☐ Cleared personnel required

Period of performance, if known

Customer / Government contracting office

32 What would you like FEDFORTRESS to deliver?

☐ Assessment / findings report☐ Site survey / discovery report☐ Architecture / design☐ Bill of materials / product selection☐ ROM / budgetary estimate☐ Formal proposal / quote☐ Implementation / integration☐ Hardened baseline / configuration☐ Scans / STIGs / technical evidence☐ RMF / authorization artifacts☐ SOPs / runbooks / procedures☐ Training / knowledge transfer☐ Software / source code / deployment package☐ O&M / sustainment support☐ Other deliverable

Other deliverable or acceptance criteria

33 Customer-furnished information available

☐ SOW / PWS / SOO / requirements☐ RFI / RFQ / RFP package☐ Network / architecture diagrams☐ Hardware / software inventories☐ Current configurations / baselines☐ Scan results / STIG checklists☐ RMF / eMASS artifacts☐ Floor plans / facility drawings☐ Non-sensitive photos / site documentation☐ License / support information☐ Existing BOM / quotes☐ As-builts / prior design docs

Important assumptions, customer responsibilities, approvals, or dependencies already known



ADDITIONAL INFORMATION & SUBMISSION

34 Key constraints, risks, or decisions

What constraints, risks, blockers, or decisions should we understand before we respond?

35 Additional mission context

Anything else that would help us understand the mission, environment, stakeholders, or desired approach

36 Attachments and follow-up

List non-sensitive files you plan to provide (do not attach protected information without coordination)

Preferred next action

- | | |
|---|--|
| ☐ Schedule a discovery call | ☐ Review the provided requirements |
| ☐ Prepare a ROM / budgetary estimate | ☐ Prepare a proposal / quote |
| ☐ Discuss a site survey | ☐ Other / contact me to determine next step |

Best contact method

Best days / times

Alternate POC

SUBMITTING THIS SURVEY

For a completed survey containing only non-sensitive information, send it to contact@fedfortress.com or provide it through another method coordinated with FEDFORTRESS. If the discussion requires classified, CUI, FCI, export-controlled, proprietary-sensitive, or otherwise protected information, contact us first so an appropriate transmission and handling method can be established.

FEDFORTRESS LLC

Panama City, Florida | contact@fedfortress.com | fedfortress.com

Woman-Owned | Service-Disabled Veteran-Owned | UEI XFZ5Q9SY3Z45 | CAGE 0QJ06