INFORMATION
ASSURANCE
CAPABILITIES

Commercial Solutions for Classified

harnessing the power of commercial industry

Mobile Access Capability Package

Registration Package

Registration #

Solution Name:

Date Submitted:

Solution Name:

Commercial Solutions for Classified

Mobile Access Registration Form

Upon completion of this form, please fill appropriate overall classification and portion mark all classified fields entered.
Completed form will be at least UNCLASSIFIED//FOR OFFICIAL USE ONLY.
If completed form is classified, please contact CSfC PMO for delivery instructions.
Send complete form to csfc_register@nsa.gov.

● Initial CSfC Registration for a new CSfC Solution

○ Registration Re-submittal (for a recently submitted and unapproved CSfC Registration)

○ Existing (one-year) Registration Renewal to renew an existing and previously approved CSfC Registration

GENERAL INFORMATION	
Agency or Service Using Solution:	
Solution Name:	
Classification of Complete Form:	
Capability Package:	Mobile Access Capability Package
Capability Package Version:	
Classification of Data Processed:	
Network/Solution Location:	
Date Submitted:	
Renewal Date:	One year from Date Approved
Total # of Submitted Deviations:	

Solution Name:

OPERATIONAL POINT OF CONTACT (POC)	
Last Name:	
First Name:	
Title:	
Organization:	
Address:	
City:	
State:	
Zip Code:	
Telephone (Commercial):	
Telephone (DSN):	
Email Address (INTERNET):	
Email Address (SECRET):	
Email Address (TOP SECRET):	

ALTERNATE OPERATIONAL POC	
Last Name:	
First Name:	
Title:	
Organization:	
Address:	
City:	
State:	
Zip Code:	
Telephone (Commercial):	
Telephone (DSN):	
Email Address (INTERNET):	
Email Address (SECRET):	
Email Address (TOP SECRET):	

DESIGNATED APPROVAL AUTHORITY (DAA) or AUTHORIZING OFFICIAL (AO)	
Last Name:	
First Name:	
Title:	
Organization:	
Address:	
City:	
State:	
Zip Code:	
Telephone (Commercial):	
Telephone (DSN):	
Email Address (INTERNET):	
Email Address (SECRET):	
Email Address (TOP SECRET):	

Solution Name:

INTEGRATOR INFORMATION	
Technical POC Last Name:	
Technical POC First Name:	
Title:	
Company, Service, Agency, or Organization:	
Address:	
City:	
State:	
Zip Code:	
Telephone (Commercial):	
Telephone (DSN):	
Email Address (INTERNET):	
Email Address (SECRET):	
Email Address (TOP SECRET):	

ALTERNATE INTEGRATOR INFORMATION	
Technical POC Last Name:	
Technical POC First Name:	
Title:	
Company, Service, Agency, or Organization:	
Address:	
City:	
State:	
Zip Code:	
Telephone (Commercial):	
Telephone (DSN):	
Email Address (INTERNET):	
Email Address (SECRET):	
Email Address (TOP SECRET):	

ADDITIONAL POC (optional)	
Last Name:	
First Name:	
Title:	
Company, Service, Agency, or Organization:	
Address:	
City:	
State:	
Zip Code:	
Telephone (Commercial):	
Telephone (DSN):	
Email Address (INTERNET):	
Email Address (SECRET):	
Email Address (TOP SECRET):	

FOR EACH COMPONENT CHOSEN FROM THE CSFC COMPONENTS LIST
Please complete all fields for component entries (N/A is acceptable for us-used components).

Component Make / Model:	
Component Function:	Mobile Platform (EUD)
Component Version / Release Level:	
Number of Devices in Overall Solution (estimated):	
Deviation (Yes or No)	

Component Make / Model:	
Component Function:	VPN Client (outer)
Component Version / Release Level:	
IKE Version:	
Key Agreement Algorithm / NIST Curve:	
Peer Authentication Algorithm / NIST Curve:	
IKE SA Encryption Algorithm / Mode / Key Length:	
ESP SA Encryption Algorithm / Mode / Key Length:	
Describe the Initial Provisioning/Configuration Procedure:	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	VPN Client (inner)
Component Version / Release Level:	
IKE Version:	
Key Agreement Algorithm / NIST Curve:	
Peer Authentication Algorithm / NIST Curve:	
IKE SA Encryption Algorithm / Mode / Key Length:	
ESP SA Encryption Algorithm / Mode / Key Length:	
Describe the Initial Provisioning/Configuration Procedure:	
Deviation (Yes or No):	

Solution Name:

Component Make / Model:	
Component Function:	Dedicated Outer VPN
Component Version / Release Level:	
IKE Version:	
Key Agreement Algorithm / NIST Curve:	
Peer Authentication Algorithm / NIST Curve:	
IKE SA Encryption Algorithm / Mode / Key Length:	
ESP SA Encryption Algorithm / Mode / Key Length:	
Describe the Initial Provisioning / Configuration Procedure:	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	VoIP Application / TLS Applications(s)
Component Version / Release Level:	
TLS cipher suite to be used:	
SRTP Encryption Algorithm / Mode/ Key Length:	
Describe the Initial Provisioning / Configuration Procedure:	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	Traffic Filtering Firewall (black)
Component Version / Release Level:	
Deviation (Yes or No)	

Component Make / Model:	
Component Function:	IDS / IPS (black)
Component Version / Release Level:	
Monitoring Point:	M1
Deviation (Yes or No)	

Component Make / Model:	
Component Function:	VPN Gateway (outer)
Component Version / Release Level:	
IKE Version:	
Key Agreement Algorithm / NIST Curve:	
Peer Authentication Algorithm / NIST Curve:	
IKE SA Encryption Algorithm / Mode / Key Length:	
ESP SA Encryption Algorithm / Mode / Key Length:	
Deviation (Yes or No):	

Solution Name:

Component Make / Model:	
Component Function:	VPN Gateway (inner)
Component Version / Release Level:	
IKE Version:	
Key Agreement Algorithm / NIST Curve:	
Peer Authentication Algorithm / NIST Curve:	
IKE SA Encryption Algorithm / Mode / Key Length:	
ESP SA Encryption Algorithm / Mode / Key Length:	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	Certificate Authority (outer)
Component Version / Release Level:	
Is this a Root CA?	
If this is a Subordinate CA, identify the Root and any intermediate CAs in the chain:	
Is CA Certificate signed using ECDSA P-384, P-256 or RSA 2K Algorithms?	
Are CA issue Certificates signed with ECDSA P-384, P-256 or RSA 2K?	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	Certificate Authority (inner)
Component Version / Release Level:	
Is this a Root CA?	
If this is a Subordinate CA, identify the Root and any intermediate CAs in the chain:	
Is CA Certificate signed using ECDSA P-384, P-256 or RSA 2K Algorithms?	
Are CA issue Certificates signed with ECDSA P-384, P-256 or RSA 2K?	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	Traffic Filtering Firewall (gray)
Component Version / Release Level:	
Deviation (Yes or No)	

Component Make / Model:	
Component Function:	IDS / IPS (gray)
Component Version / Release Level:	
Monitoring Point (M2 or M4):	M2
Deviation (Yes or No)	

Solution Name:

Component Make / Model:	
Component Function:	SRTP/TLS Encryption Endpoint (i.e. SIP Server, Session Border Controller)
Component Version / Release Level:	
TLS cipher suite to be used:	
SRTP Encryption Algorithm / Mode/ Key Length:	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	TLS Server (inner)
Component Version / Release Level:	
TLS cipher suite to be used:	
Deviation (Yes or No):	

Component Make / Model:	
Component Function:	Traffic Filtering Firewall (red)
Component Version / Release Level:	
Deviation (Yes or No)	

Component Make / Model:	
Component Function:	IDS / IPS (red)
Component Version / Release Level:	
Monitoring Point:	M3
Deviation (Yes or No)	

Component Make / Model:	
Component Function:	
Component Version / Release Level:	
Deviation (Yes or No)	
Additional Info:	

Component Make / Model:	
Component Function:	
Component Version / Release Level:	
Deviation (Yes or No)	
Additional Info:	

Does the planned Mobile Access solution also involve secure web and / or e-mail?	

Does the planned Mobile Access solution also involve a Data-at-Rest Solution / Registration?	

Solution Name:

How is Policy enforcement achieved? If using MDM, list component name and version number. If by other means, please describe.	

Describe the Black Transport:	

Briefly, (in 2-3 sentences) describe how this CSfC solution meets the operational mission objectives. Also, please specify how many end-users will be supported by the CSfC solution:

General Comments:

APPROVING OFFICIAL SIGNATURE REQUIRED
Please select the applicable statement

By signing below the AO is asserting compliance with the published Mobile Access CP and acknowledges / accepts the risk of fielding a CSfC solution.

X

Date ________________

By signing below, the AO acknowledges enclosing the Mobile Access CP Deviation Approval Letter signed by NSA and acknowledges / accepts the risk of fielding a CSfC solution.

X

Date _________________