

GCSS-A v2.1 RS 1.1 ATO Approval (UNCLASSIFIED)
From: Winkler, Gary L Mr CIV USA USAASC [gary.winkler@us.army.mil]
Sent: Wednesday, April 27, 2011 2:25 PM
To: Domke, Timothy LTC MIL US USA; McKinnon, Bobby L Mr CIV USA USAASC;
Halstead, Matthew Mr CIV US USA USAASC; Lee, Lisa A Mrs CIV USA
USAASC; Parrish, Rosalynn CIV USA; Wheatley, Kevin CIV USA; Bezwada,
Hari CIV USA; Watson, Terry SES CIV USA USAASC; Ullah, Anm S CIV US USA;
Flanders, Thomas P COL MIL USA USAASC
Subject: GCSS-A v2.1 RS 1.1 Change Approval (UNCLASSIFIED)
Signed By: WINKLER.GARY.L. 1027842409

Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

LTC Domke,

I granted an ATO for GCSS-A v2.0 RS 1.1 effective 5 Jul 2010 with the following contingency:

* Due to the rapid deployment of changes for this system I approve an ATO for all GCSS-A v2.x that meet the following requirements:

* All GCSS-Army v2.x changes must be made available for DAA Accreditation impact assessment prior to their initial implementation and throughout the GCSS-Army v2.x life cycle. DAA approved GCSS-Army v2.X minor changes shall not require a new ATO. This ATO requires revalidation if major changes or upgrades are applied to the baseline configuration, architecture or implementation. DAA approved GCSS-Army v2.X minor changes shall not affect the current Authorization Termination Date (ATD).

My staff has reviewed the documentation submitted in support of your request for a version change. An Application Certificate of Networkiness (CoN) for the Stunnel encryption was also submitted to Networkiness for approval. Based on my staff's recommendation and once a CoN is received, I approve the tested SAP GUI for Java with Stunnel as the FIPS 140-2 compliant encryption to be fielded as GCSS-Army v2.1 RS 1.1 with no impact to the ATD of 4 Jul 2013.

Prior to fielding, please update all DIACAP artifacts with the new version and incorporate all system changes within the documentation.

My point of contact for this action is Lisa Lee, Information Assurance Program Manager (IAPM), 703-806-0962.

Gary L. Winkler
Program Executive Officer

-----Original Message-----

From: Winkler, Gary L Mr CIV USA USAASC [mailto:gary.winkler@us.army.mil]
Sent: Wednesday, June 30, 2010 4:22 PM
To: Wilson, Jeffrey K COL MIL US USA; Ullah, Anm S CIV US USA; Assi, Carol M

Ms CIV USA CIO/G-6; Muhammad, James D Mr CTR US USA CIO/G-6; Lee, Kevin F CIV USA AMC; Zilinski, David A CIV USA AMC; Dixon, Sally A Ms CIV USA CIO/G-6; Moore, John K CIV USA NETCOM/9TH SC A 7TH SC; Lyday, Sandra CIV USA NETCOM/9TH SC A 7TH SC; McDonald, Justine E CIV USA NETCOM/9TH SC A 7TH SC; Springer, Bryant MAJ MIL USA; iacora@us.army.mil; Alvarez, Sandra D Mrs CIV USA USAASC; Love, Lisa Ms CIV USA USAASC; Browell, Thomas C Mr CIV US USA USAASC; Smith,

GCSS-A v2.1 RS 1.1 ATO Approval (UNCLASSIFIED)

Tracy CIV USA AMC; Kessler, John G CTR US USA; Asare, Bernard CTR US USA; Smith, Garold A Mr CTR US USA NETCOM/9TH SC A; Van Winkle, Robert E Mr CIV USA NETCOM/9TH SC A 7TH SC; Chew, David B Mr CTR US USA CIO/G-6; Mullin, Judi L Ms CIV USA AMC; Mick, Leonard G CIV USA NETCOM/9TH SC A 7TH SC; Barrett, Gerald S Mr CIV USA NETCOM/9TH SC A; Houst, Peter J CIV USA NETCOM/9TH SC A 7TH SC; Tanner, Robert D CIV USA USAASC; Vega, Rachel F Ms CIV US USA CIO/G-6; Davis, Shonda L Ms CTR US USA CIO/G-6; Johnson, Arthur J CTR US USA; Stephens, Cepion F SFC MIL USA NETCOM/9TH SC A; Barry, Phillip S MSG MIL USA; Ford, Lonye N Ms CTR US USA; Chasteen, Gregory T CIV USA
Subject: GCSS-A v2.0 RS 1.1 ATO (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

ET-IA-181-1

COL Jeffery Wilson,

I agree with the CA recommendation below; I assume the operational risk; and I approve an ATO for GCSS-A v2.0 RS 1.1 at the MAC II Sensitive Level effective 5 Jul 2010 with an ATD of 4 Jul 2013.

In accordance with the requirements of Chairman Joint Chief of Staff Instruction (CJCSI) 6211.02C, Defense Information System Network (DISN): Policy, Responsibilities and Processes, 09 July 2008, and System/Network Approval Process (SNAP) Requirements, I acknowledge and consent to DISA conducting initial and periodic unannounced vulnerability assessments and compliance monitoring scans of my connected host network.

A Security Test and Evaluation (ST&E) was conducted on the Global Combat Support System - Army version 2.0 Release 1.1 (GCSS-A v2.0 RS 1.1) and the findings established that the overall system risk meets the standards described in AR 25-2. I have reviewed the information concerning this request and with consideration of the recommendations provided by my staff; I concur

with the assessment of the risk. This risk has been weighed against the operational requirements and security measures that have or will be implemented in the area of physical, personnel, hardware, software, procedural, and communications security.

GCSS-Army v2.0 RS 1.1 is designed to meet DODI 8500.2 IA controls for integrity and availability (I & A) at the MAC II level and confidentiality at the SENSITIVE level.

This ATO is contingent on the following provisions:

- * PM GCSS-Army will comply with all caveats in the CA Recommendation for GCSS-A v2.0 RS 1.1 dated 5 Jul 2010.
- * Federal Information Security Management Act (FISMA) requires at a minimum annual validation of security controls and contingency plans. Submit required validation documents and date the validation was performed to this office annually. FISMA requires a Plan of Action and Milestones (POA&M) that include specific tasks to mitigate vulnerabilities. Submit required POA&M to this office on a quarterly basis.
- * The PM GCSS-Army will ensure that all information assurance (IA) equipment operated/enabled software and hardware that is managed and maintained within

GCSS-A v2.1 RS 1.1 ATO Approval (UNCLASSIFIED)

the GCSS-A v2.0 RS 1.1 topology is compliant with the Army Information Assurance Approved Products List (AIAAPL) or follow implementation guidance as documented in the Letter to Industry.

* The PM GCSS-Army will ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or any other modification is reported to my point of contact for this action for review and approval prior to fielding and is analyzed through the configuration management process to determine its impact on system security.

* PM GCSS-Army will ensure compliance with all operational and Information Assurance guidance published by JTF-GNO, DOD, Army and PEO EIS to include applicable Communications Tasking Orders (CTOs), INFOCONS and ALARACTS.

* Due to the rapid deployment of changes for this system I approve an ATO for all GCSS-A v2.x that meet the following requirements:

* All GCSS-Army v2.x changes must be made available for DAA accreditation impact assessment prior to their initial implementation and throughout the GCSS-Army v2.x life cycle. DAA approved GCSS-Army v2.X minor changes shall not require a new ATO. This ATO requires revalidation if major changes or upgrades are applied to the baseline configuration, architecture or implementation. DAA approved GCSS-Army v2.X minor changes shall not affect the current Authorization Termination Date (ATD).

My point of contact for this action is Lisa Love, Information Assurance Program Manager (IAPM), 703-806-2143.

Gary L. Winkler
Program Executive Officer

-----Original Message-----

From: Assi, Carol M Ms CIV USA CIO/G-6 [mailto:Carol.Assi@us.army.mil]

Sent: Tuesday, June 29, 2010 5:52 PM

To: Winkler, Gary L SES CIV USA

Cc: Wilson, Jeffrey K COL MIL US USA; Tanner, Robert D CIV USA USAASC; Love,

Lisa Ms CIV USA USAASC; Smith, Tracy CIV USA AMC; Muhammad, James D Mr CTR

US
USA CIO/G-6; Dixon, Sally A Ms CIV USA CIO/G-6; Vega, Rachel F Ms CIV US USA

CIO/G-6; Davis, Shonda L Ms CTR US USA CIO/G-6; Chew, David B Mr CTR US USA

CIO/G-6; Mullin, Judi L Ms CIV USA AMC; Mick, Leonard G CIV USA NETCOM/9TH

SC
A 7TH SC; Barrett, Gerald S Mr CIV USA NETCOM/9TH SC A; Van Winkle, Robert E

Mr CIV USA NETCOM/9TH SC A 7TH SC; Houst, Peter J CIV USA NETCOM/9TH SC A

7TH
SC; Johnson, Arthur J CTR US USA; Lyday, Sandra CIV USA NETCOM/9TH SC A 7TH

SC; McDonald, Justine E CIV USA NETCOM/9TH SC A 7TH SC; Springer, Bryant MAJ

MIL USA; Smith, Garold A Mr CTR US USA NETCOM/9TH SC A; Stephens, Cepion F

SFC
MIL USA NETCOM/9TH SC A; Barry, Phillip S MSG MIL USA

Subject: GCSS-A v2.0 RS 1.1 ATO (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Sir,

Please document your approval by cutting and pasting the following statement

GCSS-A v2.1 RS 1.1 ATO Approval (UNCLASSIFIED)

with your digitally signed reply and your signature block:

I agree with the CA recommendation below; I assume the operational risk; and I approve an ATO for GCSS-A v2.0 RS 1.1 at the MAC II Sensitive Level effective 5 Jul 2010 with an ATD of 4 Jul 2013.

BLUF: As the Army Certification Authority (CA), I recommend that you, as the DAA, assume the operational risk, consent to DISA performing vulnerability assessments, and approve an Authorization to Operate (ATO) the Global Command Support System - Army version 2.0 Release 1.1 (GCSS-A v2.0 RS 1.1) at the MAC II Sensitive Level effective 5 Jul 2010 with an Authorization Termination Date (ATD) of 4 Jul 2013. I have confirmed this recommendation with my digital signature and request that you confirm your approval of this ATO with your digital signature reply on the statement above and forward a copy of the approval to IACORA@us.army.mil. The Scorecard supporting this recommendation is attached, the POA&M was sent under separate encrypted email message.

The System Owner, COL Jeffrey K. Wilson, PM GCSS-A, has requested an ATO for GCSS-A v2.0 RS 1.1, APMS# DA0133MII. GCSS-A v2.0 RS 1.1 provides Combat Service Support for tactical forces, as depicted in the attached diagram.

GCSS-A v2.0 RS 1.1 is designed to meet the DoDI 8500.2 IA controls for availability and integrity at MAC II (i.e., consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time) and for confidentiality at the SENSITIVE Level. GCSS-A v2.0 RS 1.1 introduces a LOW level of risk to the Army networks and data when implemented and operated with protection mechanisms as described in the GCSS-A v2.0 RS 1.1 Information Assurance Certification and Accreditation (IA C&A) package as updated Jun 2010.

As the Army CA, consistent with my responsibilities as the Senior Information Assurance Official (SIAO), I recommend that you assume the operational risk, consent to DISA conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments and approve an ATO for the GCSS-A v2.0 RS 1.1 effective 5 Jul 2010 with an ATD of 4 Jul 2013 with the following caveats:

* GCSS-A v2.0 RS 1.1 is implemented and operated with the protection mechanisms documented in the GCSS-A v2.0 RS 1.1 information assurance C&A package as updated Jun 2010

* The System Owner updates the APMS with the ATO information once this recommendation is approved by the DAA.

This CA recommendation is provided in support of a DAA ATO decision and requires revalidation if major changes or upgrades are applied to the

GCSS-A v2.1 RS 1.1 ATO Approval (UNCLASSIFIED)

baseline configuration, architecture or implementation or upon modification or expiration of the ATO.

Carol Assi

Army CIO/G6
Cyber/IA Directorate
Director, Office of Information Assurance and Compliance (OIA&C) Army
Certification Authority
(703) 602-7398
carol.assi@us.army.mil

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE