NATIONAL GUARD BUREAU
1411 JEFFERSON DAVIS HIGHWAY
ARLINGTON VA 22202-3231

NGB J2 19 April 2010

MEMORANDUM FOR RECORD

SUBJECT: Signed Approval of Revised Acceptable Use Policy for GIIEP

1. I hereby approve the attached revised text of the Acceptable Use Policy (AUP) for general users of the National Guard Bureau (NGB) Geospatial Information Interoperability Exploitation Portable (GIIEP) system.

2. The attached policy will be in effect indefinitely until this office publishes amendments or changes to the current text.

3. POC for this Memorandum is the undersigned at phone 703-604-4237 or email terry.quist@us.army.mil.

Terry C. Quist
TERRY C. QUIST
LTC, MI
Acting Chief,
NGB J2 Plans, Policies, and Programs Division

Geospatial Information Interoperability Exploitation - Portable (GIIEP)

Acceptable Use Policy (AUP)

1. **Purpose.** Controls are needed for GIIEP to ensure all users are accountable for their own actions and to protect mission-related data and equipment from either malicious and accidental loss or damage. The following AUP has been developed to govern the behavior of GIIEP users to ensure they know and accept their responsibilities with respect to GIIEP security. Individuals must agree to conform to these rules. This will be accomplished during the GIIEP user registration process prior to being provided GIIEP access. Consequences for violating the AUP vary according to the seriousness of the violation.

2. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the GIIEP from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

3. **Access.** Access to the GIIEP is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

4. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

5. **Classified Information Processing**. The GIIEP is an Unclassified FOUO Information System (IS) supporting the National Guard Bureau (NGB) mission. The GIIEP is also a US-only system and approved to process only up to Unclassified / FOUO information in accordance with the current accreditation document.

   a. The GIIEP not accredited for transmission of NATO material.

   b. The ultimate responsibility for ensuring the protection of information lies with the user. The release of classified information through the GIIEP is a security violation and will be investigated and handled as a security violation or as a criminal offense.

6. **Unclassified / FOUO information processing**. The GIIEP is authorized to process Unclassified / FOUO information.

7. **Minimum security rules and requirements.** As a GIIEP system user, the following minimum security rules and requirements apply:

a. I understand personnel are not permitted access to GIIEP unless in complete compliance with the DOD and Army personnel security requirements. At a minimum, the standards for an IT-III position, as stated in AR 25-2, will be met. In addition, I confirm that my access to GIIEP is required to fulfill need-to-know requirements

b. I have completed required security awareness-training (DoD Personnel, non-DoD Personnel). Proof of security awareness training will be provided prior to granting access to GIIEP. I will participate in all training programs as required by the GIIEP IASO (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect my password. I am the only authorized user of this account. I will not use your user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords. Your password will meet the following requirements:

- It must be at least 15 characters
- It must contain at least 2 special characters: !@#$%^&*_-+=':;.,
- It must contain at least 2 numbers
- It must contain at least 2 uppercase and 2 lowercase letters
- It must not be one of your last 10 passwords.
- It IS case sensitive

d. When accessing GIIEP form a DoD/Army network I will use only authorized hardware and software to include wireless technology. I will not install or use any personally owned hardware, software, shareware, or public domain software on government furnished equipment.

e. To protect GIIEP against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb storage device, or other storage media.

f. I will not attempt to access or process data exceeding GIIEP's authorized classification level, which is Unclassified / FOUO.

g. I will not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize ARNG/Army/DOD provided ISs for commercial financial gain or illegal activities.

k. I understand that GIIEP maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the SA and /or the information Assurance Security Officer (IASO) and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to GIIEP IASO.

o. I understand that monitoring of GIIEP will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions. I understand that the following activities are prohibited uses of GIIEP:

- Unethical use (e.g. Spam, profanity, sexual misconduct, gaming, extortion)
- Introducing unauthorized services to the GIIEP architecture (e.g. peer-to-peer, distributed computing)
- Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams)

p. I understand that I do not have a recognized expectation of privacy in official data when logged on to GIIEP and may have only a limited expectation of privacy with regards to personal data on the GIIEP. I realize that I should not store data on GIIEP that I do not want others to see.

q. I will scan all files for malicious software (e.g., viruses and worms) prior to introducing them to GIIEP.

r. I will not transfer information using magnetic media from a classified system to GIIEP.

7.1 USB AUP

7.1 USB Acceptable Use Policy (AUP)

a. Users are allowed to use only the following USB devices on the GIIEP system

JVC	GZ-MS120	Everio S GZ-MS120 Camcorder
AverMedia	C038	DVD EZMaker USB Gold Capture Card
SanDisk	SDSDRH-016G-A11	16GB SD Memory Card
Ricoh	500ES-W	Still Camera
Ricoh	SE-2G	GPS Module

Iridium	9555	9555 Satcom Phone

b. Use of authorized government-owned flash SIMS devices with personal or other unauthorized computers is not allowed. Only the USB devices listed above will be allowed on GIIEP systems.
c. Any replacement SIM must be disk wiped using a DoD approved tool before first use and then scanned using Symantec anti-virus (Ghost).
d. Access control to the SIM is through the CF30 laptop using Army Regulation 25-3 password policies.
e. Power down volatile memory devices for 60 seconds before connecting to any endpoint.
f. Non-government owned USB devices WILL NOT be connected to the GIIEP system.
g. Disguised USB devices WILL NOT be used.
h. Label and handling instructions should follow DoD guidelines for unclassified material.

8. **By signing this document, you acknowledge and consent that when you access GIIEP**:

a. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

b. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

(5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counter intelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(b) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(c) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(d) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(e) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counter intelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless o whether the banner expressly references this User Agreement.

9. **Acknowledgement.** The authority for soliciting your Social Security Number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to (insert your organization) information systems. I have read the above requirements regarding use of (insert your organization) access systems. I understand my responsibilities regarding these systems and the information contained in them.

______________________________ ___________________________
Directorate/Division/Branch/Unit Date

______________________________ ___________________________
Last Name, First, MI Rank/Grade SSN

______________________________ ___________________________
Signature Phone Number