UNCLASSIFIED/FOUO		
ONE-NET BLACKBERRY USER AGREEMENT		
NOTE: This information may be used to contact a Blackberry user in the event of a security incident or an emergency.		
PRIVACY ACT STATEMENT		
AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Identifies the user of the BlackBerry device as receiving usage and security awareness training governing use of the device and agreeing to use the device in accordance with security and wireless policies. The information is used for inventory control of the device and to verify compliance with DoD requirements regarding accountability of information processing systems, and provides emergency contact information on the user in the event that the device becomes lost, stolen, otherwise compromised, or requires a reconfiguration due to security policy changes. **ROUTINE USE(S)**: None. **DISCLOSURE**: Voluntary; however, failure to provide the requested information will result in denial in issuance of a Blackberry device.		
PART I - PERSONAL INFORMATION		
1. LAST NAME	2. FIRST NAME	3. MIDDLE INITIAL
4. RANK/RATE	5. ORGANIZATION	6. DEPARTMENT/DIVISION
7. BUILDING NUMBER	8. ROOM NUMBER	9. WORK TELEPHONE NUMBER
10. E-MAIL ADDRESS		
PART II - BLACKBERRY INFORMATION		
11. DEVICE(S) MAKE, MODEL, AND SERIAL NUMBER		
12. The following preventive measures are requirements to ensure that the use of the BlackBerry device does not result in the release of DoD information to unauthorized persons.		

DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," 9 May 2008 Requirements:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- 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.
- You consent to the following conditions:
  - 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, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this information system.
  - 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.
  - 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.
  - 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:

- 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 network 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 counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
- 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.
- 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.
- 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.
- 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.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence 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.
- 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 provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

The following additional requirements apply to all users of the Blackberry device:

a. I agree that this device is used only for end-user type access to information systems and controlled unclassified information and below, and is not to be used to send, receive, store, or process classified information. It will not be connected to any system processing classified information without the written approval of the Designated Approving Authority (DAA).

b. I acknowledge that this BlackBerry device is not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facilities (SCIFs) unless approved by the SCIF Cognizant Security Authority (CSA), and is not allowed in areas where classified information is stored, transmitted, or processed.

c. I will immediately report the loss of this device to the site Information Assurance Manager/Information Assurance Officer (IAM/IAO) and the LNSC Director to ensure that appropriate response procedures can be initiated.

d. I may be held responsible for damage caused to this government system or data through negligence or a willful act.

e. I will turn my Blackberry device in to be checked on a quarterly basis to the Site Blackberry Administrator to ensure compliance with standard load configuration and applicable security policies.

f. I understand that if the Blackberry device is involved or suspected to be or have been involved in or with Classified Message Incident (CMI), I am required to immediately contact the IAM/IAO and surrender my device for further investigation, including incidents involving the receipt and transmission of malicious codes.

g. I understand that my Blackberry device is required to be fully synchronized with the Blackberry Server at a minimum of once every 30 days and failure to comply may result in my Blackberry service account being disabled. Note: To ensure a full sync takes place, you need log into your Blackberry device and allow it to sync with your Microsoft Outlook and Blackberry Server.

h. I understand that I am required to use my Common Access Card (CAC) with the Blackberry for any messages, which requires digital signature or encryption.

i. I understand that I am not authorized to make any configuration changes or modify security settings of the device. I am required to request and coordinate any configuration changes through the Site Blackberry Administrator.

j. I understand that my Blackberry device is government-owned hardware and software used for official duties only and I am the only individual authorized to use this Blackberry.

k. I understand that failure to comply with the provisions outlined above may constitute a security or policy violation resulting in forfeiture of access and possible disciplinary action.

FOR REPORTING PROBLEMS OR TO ASK QUESTIONS, CONTACT:

NCTS-FE Enterprise Service Desk (ESD): 243-3883
Site Blackberry Administrator:
Site Information Assurance Manager/Information Assurance Officer:
LNSC Director:

PART III - BLACKBERRY END USER ACKNOWLEDGEMENT

By signing this document, I am acknowledging that I accept and will abide by all the terms and conditions described above and confirm my awareness of the risks and proper procedures in the use, operation, and information security requirements of the Blackberry device.

13. SIGNATURE OF USER	14. DATE SIGNED (YYYYMMDD)

UNCLASSIFIED/FOUO