DEPARTMENT OF THE ARMY
U.S. ARMY USACE OF ENGINEERS
441 G STREET NW
WASHINGTON, D.C. 20314-1000

AUG 3 0 2013

CECI-E

CHIEF INFORMATION OFFICER'S POLICY MEMORANDUM 13-002

SUBJECT: Policy on Acquiring U.S. Army Corps of Engineers (USACE) Wireless Internet (Wi-Fi) Capabilities for Public Use at USACE Projects

1. References.

a. Chief Information Officer (CIO) Policy Memorandum 11-008, Wireless Networks and Access Points, 24 May 2011.

b. Department of Defense Information Systems Agency (DISA) Wireless Local Area Network (WLAN) Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG), Version 6, Release 5, 28 Oct 2011. Click the link below to access the STIG:
https://aceit.usace.army.mil/ACEIT%20Documents/Operational%20Directives/WLAN_AccessPointSTIG_(Internet%20Connection).pdf

c. Engineer Regulation ER 1130-2-550, Project Operations - Recreation Operations and Maintenance Policies, 15 November 1996, with Changes through 18 January 2013:
http://140.194.76.129/publications/eng-regs/ER_1130-2-550/toc.htm

2. Purpose. The purpose of this memorandum is to establish a policy for acquiring wireless Internet (Wi-Fi) capabilities for public use at USACE projects including but not limited to Project Site Areas (PSAs)[1] and locks/dams. This policy does not include USACE wireless network connections used to connect devices directly to the CorpsNet production network for USACE personnel, which is implemented pursuant to the USACE standard solution and policy described in ref 1.a. The USACE CorpsNet production network standard solution will not be made available to project guests.

3. Policy.

a. Development of Wi-Fi capabilities for public use at USACE projects is authorized, subject to review and compliance with the requirements herein and applicable regulations and statutes.

[1] PSAs are recreation areas and include campgrounds, day use areas, multipurpose areas, land and water access points (developed), marinas and/or resorts (which can also be a lease within an existing recreation area as opposed to a separate management unit), scenic viewing areas, and visitor centers.

b. Projects wishing to provide public access Wi-Fi capabilities will obtain life-cycle services and equipment from 3rd-party vendors with assistance from their local IT Chief.

c. PSAs that charge fees will follow reference 1.c., Chapter 9, Recreation Use Fees, in setting Wi-Fi use fees. The managing Division will review and consider for approval all Wi-Fi use fees.

d. All customers will be required to accept a USACE guest Wi-Fi user agreement, via a "welcome" access screen, to access the project Wi-Fi, see agreement in Appendix A. If USACE Computer Incident and Response (CIRT) personnel are called upon to investigate Internet abuse, the local site will pay for their services.

e. Each project will develop a written Standard Procedure to create, process, distribute, change and protect passwords, obtain applicable funding, and enforce signing of the user agreement. One password will be provided to all users for a defined period.

4. All scopes of work for contracts with 3rd-party vendors will include the following provisions, in addition to the required contract clauses:

a. Implement Wi-Fi Protected Access level 2 (WPA2) encryption per reference 1.b, STIG ID Number WIR0121 to ensure the access point has adequate security functionality and can implement the latest Wi-Fi Alliance IEEE 802.11 standard.

b. Implement and maintain a password for the access point per reference 1.b, STIG ID Number WIR0122. Passwords must be changed every 30 days at a minimum.

c. The systems must never be physically connected to any government networks.

d. Default admin passwords and service set identifier (SSID) names and keys must be changed from factory settings IAW reference 1.b, STIG ID Numbers NET0240 and WIR0105, respectively. Admin passwords must be changed every 90 days at a minimum.

e. The router/access point must be configured in such a manner to prevent connections to the device and associated devices initiating from the Internet. Specifically:

(1) Remote management access to the device from the Internet must be limited to a particular IP address and require remote authentication. Reference 1.b, STIG ID NET1637.

(2) Internet Control Message Protocol (ICMP) requests from Internet to the device are blocked.

(3) Port forwarding from the Internet through the device must be disabled.

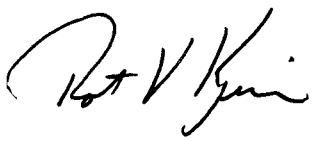
(4) Devices must be physically secured to prevent misuse similar to other network devices.

(5) Devices must be installed at least 10 meters from of any project location that processes classified National Security Information (NSI).

f. The Internet service provider (ISP)/vendor must accept all risks associated with laws and policies regarding malicious use of public internet gateways. The ISP/vendor will implement a "splash page" requiring the customer to accept the user agreement before connecting to the Internet (see Appendix A).

5. This policy is in effect immediately until withdrawn. Questions should be directed to Pep Persio, Recreation Program Manager, CECW-CO, 202-761-0036 or Jack Cicone, Telecommunications Program Manager, CECI-E, 412-395-7412.

FOR THE COMMANDER:



ROBERT V. KAZIMER
Director, Corporate Information

Encl

CF:
CEIT-ZA (Mr. Yarbro)

APPENDIX A

USACE Project and Recreation Facility Guest Wi-Fi User Agreement

This agreement ("Agreement") between you, and the Project or Recreation Facility (Facility) and Internet Service Provider (ISP) governs your access to and use of this Wi-Fi Service (the "Service"). Only current guests of the Facility may use the Service. BY ACCEPTING THIS AGREEMENT, OR BY ACCESSING OR USING THIS SERVICE, YOU REPRESENT THAT YOU ARE CURRENTLY A GUEST OF THE FACILITY AND ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO THEM. Furthermore, you agree that when you access this service you will be the sole user and that you will not allow others to use the service without their first separately reviewing and accepting this agreement.

1. AUTHORIZED USE OF THIS SERVICE. You agree that you will use this Service solely while you are a guest of this Facility, and that you are subject to the terms and conditions of this Agreement. YOU AGREE THAT YOU ARE FULLY RESPONSIBLE FOR YOUR ACTIVITIES WHILE USING THIS SERVICE (INCLUDING FOR ANY CONTENT, INFORMATION, AND OTHER MATERIALS YOU ACCESS OR TRANSMIT VIA THIS SERVICE), AND THAT YOU SHALL BEAR ALL RISKS REGARDING USE OF THIS SERVICE. YOU AGREE NOT TO USE THIS SERVICE TO ENGAGE IN ANY PROHIBITED CONDUCT. "Prohibited Conduct" is any conduct that is unlawful, infringing (such as downloading copyright protected material without the owner's permission), intentionally harmful, or otherwise of a nature that a reasonable individual should know would violate another party's rights; or conduct that otherwise interferes with the operation of, use of, or enjoyment of, any service, system or other property. By way of illustration and not limitation, prohibited conduct includes using this service to:

a. Intercept, divert or otherwise interfere with any communication,

b. Violate the security of, or gain unauthorized access to, this Service or any other communication system;

c. Impose an unreasonable or disproportionately large load on any systems or infrastructure;

d. Send "spam", chain letters, or other unsolicited communications to any party;

e. Create a "mail drop" for such communications, or engage or permit e-mail relay services;

f. Impersonate any other party, or otherwise misrepresent your identity or affiliation in any way;

g. Commit fraud;

h. Harass, or threaten any party, or encourage violence against any government, organization, group, individual or property, or provide information or assistance in causing or carrying out such violence;

i. Disseminate viruses, Trojan horses, or other code or programming intended to damage, interfere with, intercept or expropriate any system, data or personal information;

j. Send or receive any material that could be considered harmful, obscene, pornographic, indecent, lewd, violent, abusive, profane, insulting, threatening, harassing, hateful or otherwise objectionable;

k. Send or receive any material that harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, race, ethnicity, sexual orientation, gender, age, or disability;

l. Send or receive material containing defamatory, false, or libelous material;

m. Send, receive, download or print any material that infringes or violates any rights of any entity or person, including, without limitation, copyrights, patents, trademarks, laws governing trade secrets, rights to privacy, or publicity;

n. Send or receive material that you do not have a right to (for example, it was not paid for);

o. Assist others in engaging in Prohibited Conduct.

p. The Facility requires and expects that you will be a good Internet citizen and use good judgment when using this Service.

2. CONSEQUENCES OF UNAUTHORIZED USE. Without limiting any other available right or remedy, the Facility and the ISP reserve the right to, and you agree that, the Facility and/or the ISP shall have the right, to: (i) take actions they deem appropriate to protect against violations of this Agreement or abuse of the Service and to otherwise protect its interests (e.g., removing offending material, blocking access, and suspending service), and (ii) investigate immediately and cooperate with appropriate authorities regarding any actual or suspected unauthorized activities involving this Service. You agree that you will be liable to the Facility and the ISP for any damages incurred or amounts that are required to be paid by the Facility and/or the ISP that arise out of, or are related to, your violation of this Agreement. USACE reserves the right to monitor or intercept transmissions via this service for lawful purposes and to disclose such information in cooperation with legal authorities, and as otherwise required to protect rights and interests.

3. YOU ARE RESPONSIBLE FOR YOUR SECURITY AND PRIVACY. There are privacy and security risks associated with wireless communications and the Internet in general and you acknowledge that the Facility and the ISP make no assurances that your communications, or activities while using the Services, will be (or will remain) private or secure, and you further agree that the Facility and the ISP assume no responsibility in that regard. You agree that you are solely responsible for your own privacy and security in using this Service, and for

implementing appropriate measures to protect and secure your privacy, and your hardware, software and systems.

4. DISCLAIMER OF WARRANTY. YOU AGREE THAT THIS SERVICE IS PROVIDED SOLELY AS A CONVENIENCE TO GUESTS, "AS IS" AND "AS AVAILABLE." The Internet contains materials and information that may be offensive to you. You agree that you assume full responsibility and risk of use of the Services and the Internet, and that you are solely responsible for evaluating the suitability, appropriateness or legality of any content or materials you may encounter online.

5. LIMITATION OF THE FACILITY'S AND THE ISP'S LIABILITY. You agree that this service is provided as a guest privilege, SOLELY FOR YOUR CONVENIENCE, and that the use of the service does not impose liability of any kind (or in any amount) on the facility or the ISP, including without limitation, liability for any direct or indirect consequences (including, without limitation, business interruption, loss of data or profits, or other similar damages) arising out of or related to this agreement or this service even if the Facility or its ISP is advised of the possibility of any such damages.

6. TERMINATION OF SERVICE; UPDATES TO THIS AGREEMENT. You agree that the Facility or the ISP may, at any time and for whatever reason change, terminate, limit or suspend the Service or the terms and conditions of your access to the Service. Upon any termination, your rights to use the Service will immediately cease. The ISP also reserves the right to update or revise this Agreement at any time and you agree to read, review and acknowledge this Agreement prior to each and every use of the Service.

I have Read and Agree to thisagreement (connect to Internet) ___ Do not Accept ___