Division of State Patrol
Policy and Procedure

Number
5-15

Subject **DSP COMMUNICATIONS TOWER SITE SECURITY AND ACCESS CONTROL**	
Author/Originator Bureau of Network Engineering and Data Infrastructure	Approved by **Superintendent** Anthony L. Burrell
Records Management Statement Posted on WisDOT Internal Website (SharePoint) at https://wigov.sharepoint.com/sites/dot-dsp/policy/sitepages/home.aspx	

I. POLICY

It is the policy of the Division of State Patrol (DSP) to secure and control access to all of its communications tower sites. Authority for managing the communications tower site network and related property is provided in secs. 85.12(1) and 85.15(1), Wis. Stats. Implementing security and managing access to this critical infrastructure is vitally important to public safety communications. These processes will minimize unexpected changes from inadvertently leading to a denial of service, unauthorized disclosure of information, introduction of security vulnerabilities and other problems that could interrupt business operations or functions.

II. BACKGROUND

State Patrol communication tower sites, hereinafter referred to as DSP tower sites, comprised of an equipment building and a tower, are generally located on either State owned or leased property. The State Patrol also co-locates tower infrastructure with other public and private sector entities including, but not limited to the Department of Natural Resources (DNR), Educational Communications Board (ECB), Department of Health Services (DHS), Department of Corrections (DOC) as well as counties, utility companies and other private companies. These sites support several technologies including, but not limited to land mobile radio systems, other voice over IP (VoIP), and data networking using a variety of communications pathways.

A majority of DSP tower sites also directly support the Wisconsin Interoperable System for Communications (WISCOM) network and its infrastructure. WISCOM is a shared trunked radio system that first responders in communities across the state can use to communicate during a major disaster, large-scale incidents, or during special events that require interoperable voice radio communications. WISCOM can support multiple simultaneous conversation paths during an incident. This can dramatically increase the available communication capacity with statewide mutual aid talk groups and allow responders from any area of the state to assist another community without losing voice radio communications capabilities. DSP utilizes WISCOM for its daily mission-critical dispatching and operational activities. Controlled access to, and security of this critical infrastructure is essential to prevent unauthorized physical access to the network and its components.

III. OBJECTIVES

A. Assure proper security for all DSP tower sites.

B. Define, develop, implement, manage, and audit access controls to maintain security.

C. Define expectations, prohibitions, and notification procedures for co-locating agencies.

D. Ensure compliance with industry standards, best practices and other guidelines governing the physical security of critical infrastructure/key resources.

IV. KEY DEFINITIONS/ACRONYMS

A. Approved personnel – DSP employees or personnel authorized by DSP to perform work at DSP tower sites

B. BNEDI – Bureau of Network Engineering and Data Infrastructure

C. Co-Locating Agency – an agency whose communications equipment is installed upon or stored within a DSP tower site

D. DBM – Department of Transportation, Division of Business Management

E. DHS – Department of Health Services

F. DMA – Department of Military Affairs

G. DNR – Department of Natural Resources

H. DSP – Division of State Patrol

I. ECB – Educational Communications Board

J. OEC – Department of Military Affairs, Office of Emergency Communications

K. Support personnel – contractors supporting DSP; contractors supporting DBM, DHS, DMA, DNR, ECB, OEC or other co-located agencies performing work at DSP tower sites

L. WISCOM – Wisconsin Interoperable System for Communications

V. GENERAL PROVISIONS

A. DSP Staff Responsibilities:

1. DSP staff shall ensure that non-DSP staff adhere to the DSP entry and exit procedures, including those set out in Attachment A.

2. DSP staff shall immediately report all unauthorized/suspicious persons or activities at or near DSP tower sites. See Attachment A.

3. Only approved personnel will be allowed access to DSP tower sites.

4. Approved personnel may only enter DSP tower sites during the performance of their official duties.

5. Keys, codes, or other methods of access provided by the DSP must be secured at all times.
   a. Codes on all DSP tower site combination locks shall be spun to 0000 (four zeros) by DSP personnel immediately upon entry and exit of a DSP tower site so as to conceal the code from unauthorized parties.
   b. Sharing of keys, codes, or other methods of tower site access by DSP personnel, without the written approval of a DSP supervisor, is prohibited.
   c. Any known or suspected DSP tower site combination lock breach shall be immediately reported to a DSP supervisor.

6. Storage of non-essential materials, hardware, trash, spare equipment, etc. is not permitted at any DSP tower site without written approval of a DSP supervisor.

7. Damaged, disturbed, unusual, or other noteworthy items or conditions at a DSP tower site must be documented and promptly reported to a DSP supervisor.

8. All trash must be removed, and the site returned to an orderly condition by personnel prior to exiting the DSP tower site.

9. Interior lights must be turned off prior to leaving the DSP tower site.

10. DSP-contracted tower site inspections require at least one (1) DSP staff member to be present.

11. Permissions for DSP tower site access may be revoked at any time by DSP. All keys, codes or other access methods must be returned immediately upon

revocation of access privileges.

B. Co-Locating Agency Staff Responsibilities:

1. The co-locating agency shall adhere to the DSP entry and exit procedures. See Attachment A.

2. The co-locating agency shall immediately report all unauthorized/suspicious persons or activities at a DSP tower site. See Attachment A.

3. Any personnel requiring unescorted access to a DSP tower site shall affirm to the DSP annually they are in good standing with their employer and their employer has authorized them to perform unescorted work at DSP tower sites.

4. Only approved personnel will be allowed access to a DSP tower site.

5. All support personnel must be authorized by DSP. Once authorized, approved personnel may escort support personnel into the DSP tower site for the sole purpose of maintenance.

6. Approved personnel may only enter a DSP tower site during the performance of their official duties.

7. DSP will provide keys, codes, or other methods of entry as necessary to allow co-located agencies access to maintain their equipment. Duplication of keys or sharing of codes or other methods to access a DSP tower site is prohibited.

8. The co-locating agency will be responsible for assigning, tracking, and auditing all DSP site keys, codes or other methods of access.

9. Keys, codes, or other methods of access provided by the DSP must be secured at all times. Codes on all DSP tower site combination locks shall be spun to 0000 (four zeros) by the co-locating agency immediately upon entry and exit of a DSP tower site so as to conceal the code from unauthorized parties.

10. A co-locating agency may not replace or rekey a DSP site lock or door.

11. Locks shall not be replaced on common fences, gates, or doors by co-locating agencies.

12. DSP communications equipment, HVAC, dehydrator, UPS systems, generators, propane tanks, security cameras and OPTO22 alarm system sensor control equipment shall not be disturbed, adjusted, or changed without the approval of the DSP.

13. Storage of non-essential materials, hardware, trash, spare equipment, etc. is not permitted at any DSP tower site without written approval by a DSP

supervisor.

14. Damaged, disturbed, unusual or other noteworthy items or conditions at a DSP tower site must be reported to a DSP technical supervisor of the region by phone or e-mail upon entry or exit of the DSP tower site.

15. All trash must be removed, and the site returned to an orderly condition by personnel prior to exiting the DSP tower site.

16. Interior lights must be turned off prior to leaving the DSP tower site.

17. Co-locating agencies intending to perform maintenance on the DSP tower structure shall provide a minimum of 48-hour notice to DSP. In these instances, a DSP technician shall be on premises to support the work. Co-locating agencies, or their contractors, shall not commence any maintenance on the tower structure until a DSP technician is on premises.

18. If maintenance is to be cancelled, co-locating agencies shall provide notification to DSP as soon as practicable. In the event of an emergency, co-locating agencies requiring access to a DSP tower site shall notify DSP as soon as practicable and shall utilize the posted entry/exit procedures, if applicable.

19. DSP-contracted tower site inspections require at least one (1) DSP staff to be present.

20. For communications tower site inspections where WisDOT/DSP does not own the site, but has communications equipment in the building, co-locating agencies performing site inspections shall notify the DSP of the inspection when possible.

21. This policy does not supersede any agreements between WisDOT/DSP and other parties where specific tower security and access notification procedures are prescribed.

22. Pursuant to s. 85.15(1), Wis. Stats., DSP may revoke permissions for site access at any time. All keys, codes, or other access methods must be returned immediately upon revocation of site access privileges. If unescorted site access privileges are revoked, DSP staff will provide escorted access upon the request of the co-locating agency and will schedule such escort when it is mutually convenient. The scheduling of escorted access will be performed on a case-by-case basis.

VI. PROCEDURE

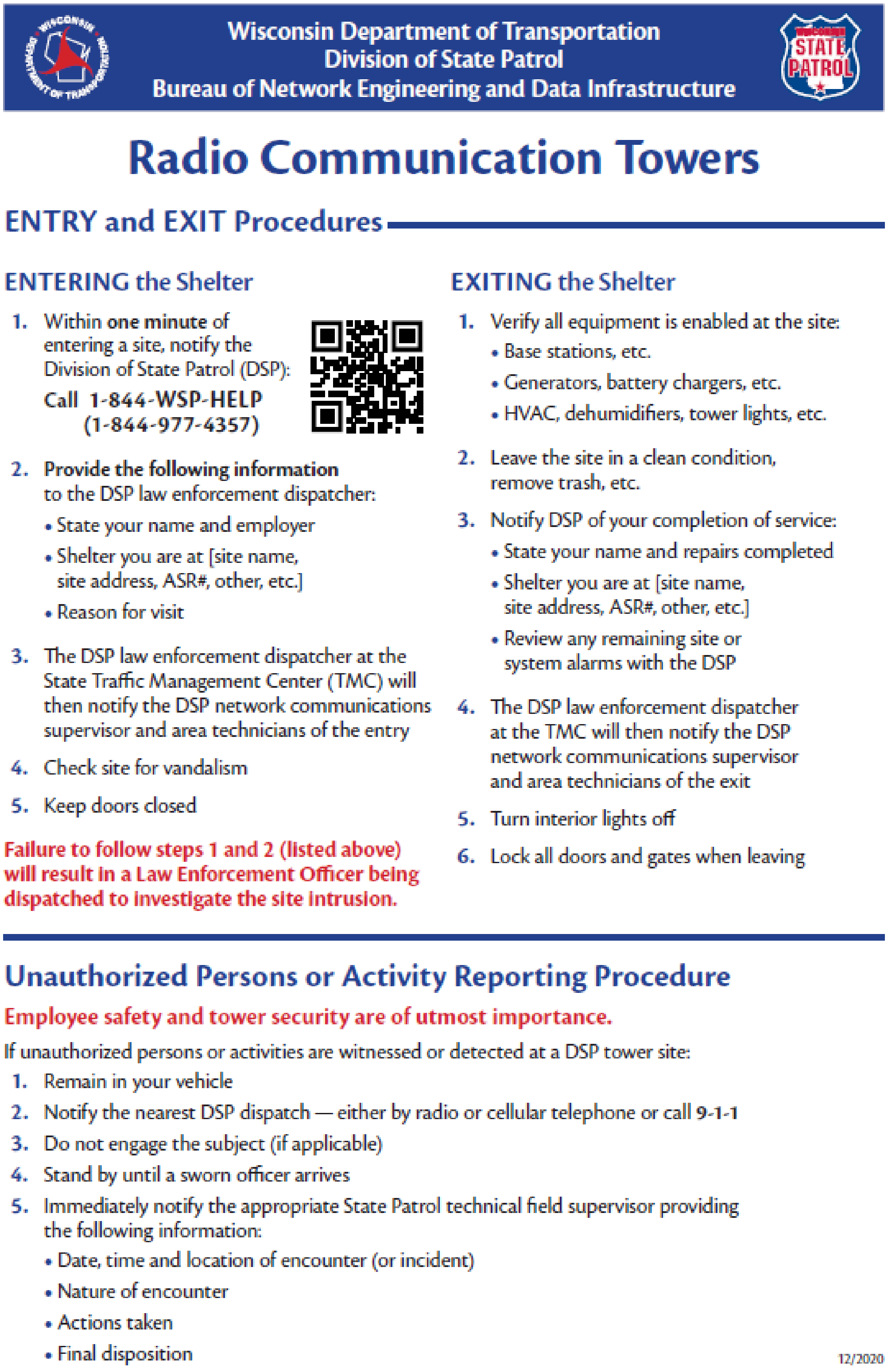
A. Pursuant to Sections V.A.(1) and V.B.(1) above, DSP staff and co-locating Agencies shall adhere to DSP entry and exit procedures as described on the Radio

Communications Tower Placard - Entry and Exit Procedures. See Attachment A.

B. Pursuant to Sections V.A.(2) and V.B.(2) above, DSP staff and co-locating Agencies shall immediately report all unauthorized/suspicious persons or activities at a DSP site as described on the Radio Communications Tower Placard - Unauthorized Persons or Activities Report. See Attachment A.

C. In addition, DSP staff will also be guided by notification procedures, methods and systems as described in Directive COM-19: Tower Entry/Exit Notification. See Attachment B.

Attachment A



Wisconsin Department of Transportation
Division of State Patrol
Bureau of Network Engineering and Data Infrastructure

Radio Communication Towers

ENTRY and EXIT Procedures

ENTERING the Shelter

1. Within **one minute** of entering a site, notify the Division of State Patrol (DSP):
   Call 1-844-WSP-HELP (1-844-977-4357)
2. **Provide the following information** to the DSP law enforcement dispatcher:
   - State your name and employer
   - Shelter you are at [site name, site address, ASR#, other, etc.]
   - Reason for visit
3. The DSP law enforcement dispatcher at the State Traffic Management Center (TMC) will then notify the DSP network communications supervisor and area technicians of the entry
4. Check site for vandalism
5. Keep doors closed

Failure to follow steps 1 and 2 (listed above) will result in a Law Enforcement Officer being dispatched to investigate the site intrusion.

EXITING the Shelter

1. Verify all equipment is enabled at the site:
   - Base stations, etc.
   - Generators, battery chargers, etc.
   - HVAC, dehumidifiers, tower lights, etc.
2. Leave the site in a clean condition, remove trash, etc.
3. Notify DSP of your completion of service:
   - State your name and repairs completed
   - Shelter you are at [site name, site address, ASR#, other, etc.]
   - Review any remaining site or system alarms with the DSP
4. The DSP law enforcement dispatcher at the TMC will then notify the DSP network communications supervisor and area technicians of the exit
5. Turn interior lights off
6. Lock all doors and gates when leaving

Unauthorized Persons or Activity Reporting Procedure

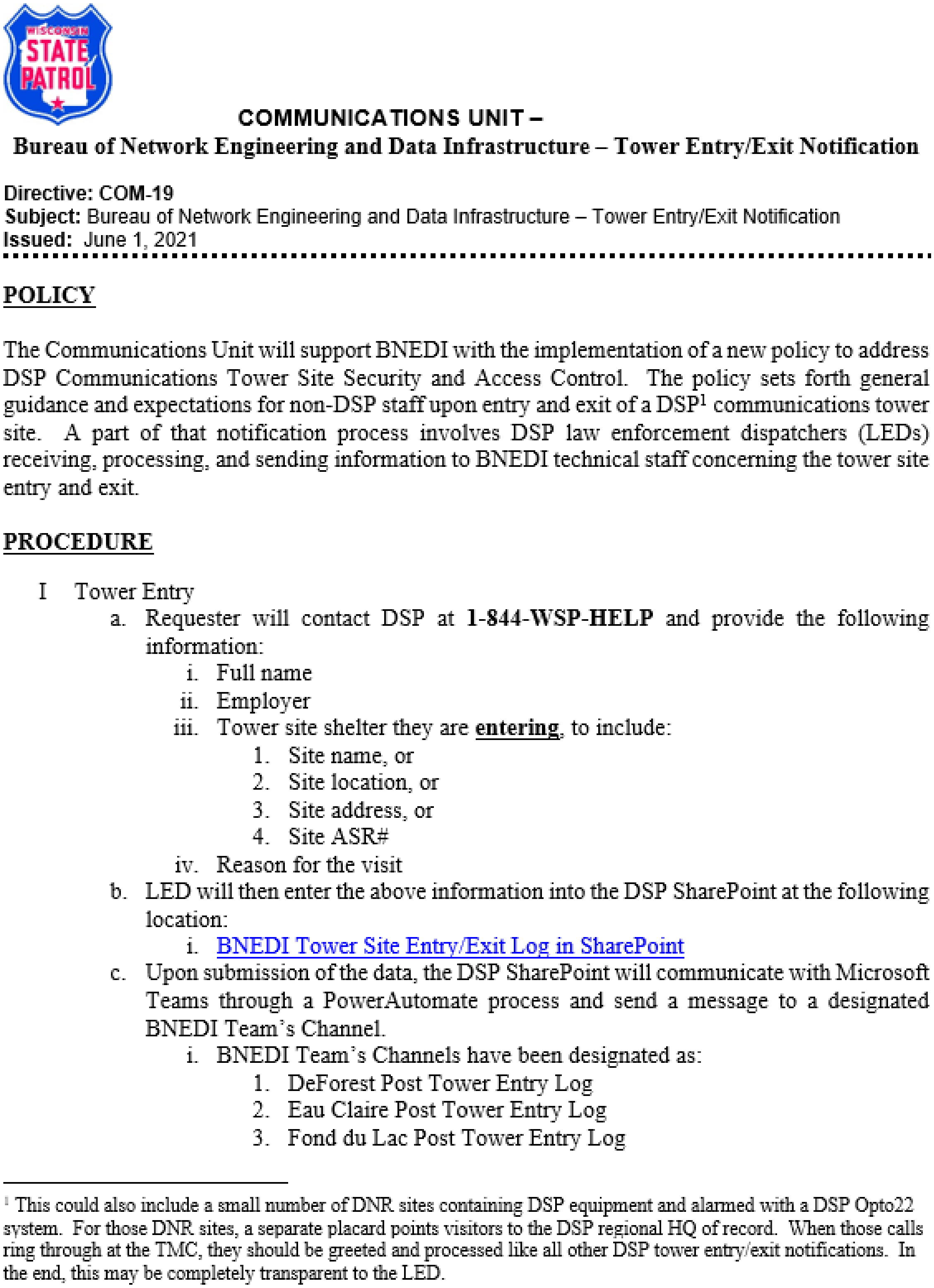
Employee safety and tower security are of utmost importance.

If unauthorized persons or activities are witnessed or detected at a DSP tower site:

1. Remain in your vehicle
2. Notify the nearest DSP dispatch — either by radio or cellular telephone or call **9-1-1**
3. Do not engage the subject (if applicable)
4. Stand by until a sworn officer arrives
5. Immediately notify the appropriate State Patrol technical field supervisor providing the following information:
   - Date, time and location of encounter (or incident)
   - Nature of encounter
   - Actions taken
   - Final disposition

12/2020

Attachment B



COMMUNICATIONS UNIT –
Bureau of Network Engineering and Data Infrastructure – Tower Entry/Exit Notification

Directive: COM-19
Subject: Bureau of Network Engineering and Data Infrastructure – Tower Entry/Exit Notification
Issued: June 1, 2021

POLICY

The Communications Unit will support BNEDI with the implementation of a new policy to address DSP Communications Tower Site Security and Access Control. The policy sets forth general guidance and expectations for non-DSP staff upon entry and exit of a DSP[1] communications tower site. A part of that notification process involves DSP law enforcement dispatchers (LEDs) receiving, processing, and sending information to BNEDI technical staff concerning the tower site entry and exit.

PROCEDURE

I Tower Entry

    a. Requester will contact DSP at **1-844-WSP-HELP** and provide the following information:
        i. Full name
        ii. Employer
        iii. Tower site shelter they are **entering**, to include:
            1. Site name, or
            2. Site location, or
            3. Site address, or
            4. Site ASR#
        iv. Reason for the visit
    b. LED will then enter the above information into the DSP SharePoint at the following location:
        i. BNEDI Tower Site Entry/Exit Log in SharePoint
    c. Upon submission of the data, the DSP SharePoint will communicate with Microsoft Teams through a PowerAutomate process and send a message to a designated BNEDI Team's Channel.
        i. BNEDI Team's Channels have been designated as:
            1. DeForest Post Tower Entry Log
            2. Eau Claire Post Tower Entry Log
            3. Fond du Lac Post Tower Entry Log

[1] This could also include a small number of DNR sites containing DSP equipment and alarmed with a DSP Opto22 system. For those DNR sites, a separate placard points visitors to the DSP regional HQ of record. When those calls ring through at the TMC, they should be greeted and processed like all other DSP tower entry/exit notifications. In the end, this may be completely transparent to the LED.

Attachment B (continued)

4. Spooner Post Tower Entry Log
5. Tomah Post Tower Entry Log
6. Waukesha Post Tower Entry Log
7. Wausau Post Tower Entry Log

d. At the same time, using the same system logic, the DSP SharePoint will also automatically communicate with enterprise e-mail through Outlook and send a companion message to a designated LED e-mail distribution list.

e. No further action is required at this time.

II Tower Exit

a. Requester will contact DSP at **1-844-WSP-HELP** and **again** provide the following information:

i. Full name
ii. Employer
iii. Tower site shelter they are **exiting**.

b. LED will then edit the time the requester left the site into the DSP SharePoint at the following location:

i. BNEDI Tower Site Entry/Exit Log - Edit

c. Upon submission of the data, the DSP SharePoint will communicate with Microsoft Teams through a PowerAutomate process and send a message to a designated BNEDI Team's Channel.

d. At the same time, using the same system logic, the DSP SharePoint will also automatically communicate with enterprise e-mail through Outlook and send a companion message to a designated LED e-mail distribution list.

e. This concludes the process.

BY ORDER OF:

Christopher Jushka, Captain
Special Operations Section

END OF DOCUMENT