

Table of Contents

Table of Contents	1
Introduction.....	1
Scope.....	2
Exceptions.....	2
Definitions.....	2
Background.....	2
Overseas Check List	3
Before You Go:.....	3
During your stay:	5
Upon your return:.....	6
Statutory Authority	6
Human Resource Implications.....	6
Related Policies, Processes, Procedures, Standards, or Best Practices.....	7
Additional Information	7
E-Mail Communications.....	7
Bluetooth.....	9
Encryption.....	10
Laptop Computer Preparations	10
Appendix 1: Sanitizing Devices for the IT Professional.	12
Appendix 2: Outlook Web Access Illustration	13
Appendix 3: Virtual Private Networks	16

Introduction

DET, in coordination with executive branch agency Information Technology and Telecommunication professionals, supports international travelers on official business. International travel is more effective as a business tool through technology and the Internet.

Risks have increased exponentially with the use of technology so reasonable steps need to be taken to mitigate risks and protect sensitive data. Smartphones, tablets and laptop computers all present security challenges to the individual and State of Wisconsin data.

International telephone and data plans vary dramatically by country. It is important to understand the components of cost when traveling to avoid extraordinary voice, text or data charges.

Scope

This checklist applies to all executive branch agencies, other than the board of regents of the University of Wisconsin System. This also includes vendors, and contractors who travel internationally for the State of Wisconsin.

Exceptions

Exemptions require the approval of the Chief Information Officer/Division Administrator Division of Enterprise Technology Department of Administration State of Wisconsin.

Definitions

The definitions for terminology in this document can be found in the Enterprise Glossary.

Background

Executive branch agencies are responsible to take reasonable and prudent steps to protect employees and sensitive information. The International Travel Addendum aids in providing information for a methodical security risk analysis. This checklist is intended to help mitigate risks to information systems and the supporting processes. Neither document is intended to replace the executive branch agencies independent judgment supporting the preparation, authorization and approval of a specific travel request and supporting technology.

Domestically, or internationally, there are two primary threat vectors or targets:

1. Theft of personal information. Criminals steal personal information for financial gain; while foreign governments might steal someone's personal information in order to gain greater access to their circle of friends or exploit one's access to company information. The software, or malware, necessary to compromise


someone's banking credentials is widely available on the internet and easier to use than ever before. Once inside a computer, moderately skilled criminal and foreign government hackers can steal credit card numbers, bank account information and other personal information stored on a user's computer or in online accounts. Hackers can also steal a person's computer resources (hard disks space, processor, internet connection) to attack other computers and evade law enforcement.

2. Theft of proprietary information. Criminals, foreign governments and foreign companies steal propriety information for monetary gain or competitive advantage. Criminals might steal a company's proprietary information in order to embarrass the company online, or hold the information for ransom. Foreign companies and governments steal proprietary information in order to gain competitive and economic advantage. They may steal recipes, manufacturing processes, legal information, trade secrets, designs, research data, corporate financial information and any other information that can be used to leapfrog into a position of comparative equality or improved market position.

Overseas Check List

BEFORE YOU GO:

- [] 1. Coordinate with your telecom manager and DOA / Division of Enterprise Technology at DOADETTelecomAdministration@wisconsin.gov or call the DOA helpdesk: (608) 267-6930 to coordinate loaned, or rented, tablets and/or cell phones. This will limit the amount of data at risk should your equipment be lost, stolen or searched. Taking personal equipment is discouraged and may pose a risk to the traveler and the State of Wisconsin.
- [] 2. Obtain a rate sheet for international charges and estimate voice, text and data expenditures for approving authority.
- [] 3. Establish device identification, (AppleID or Gmail) separate from a personal identification.
- [] 4. Obtain a copy of the procedures to follow in the event of lost or stolen equipment. This will vary based on the provider of the equipment.
- [] 5. Prepare your tablet for travel. If you cannot take a loaner device, sanitize your device by backing up the information and remove all information not needed during your travels. Ensure up-to-date protections for anti-malware, security patching and firewalls. Note: Deleting files is not sufficient to remove the information from the hard drive, consult IT staff

	Chapter: Security
	Subject: International Travel Check List

DRAFT Published: August 10, 2016

to permanently remove information not needed for travel if a sanitized loaner device is not available.

- [] 6. Minimize the information you take with you. Take the minimum amount of information needed for your travel. Do not take sensitive information (electronic or printed) with you as you travel. Evaluate the sensitivity of the information you are considering taking by knowing in many countries/cultures there is no expectation of privacy. Backup all information you do take and leave the backup at work. Remove all external storage media (e.g. CDs, USBs, etc.) from the computer before you travel.

- [] 7. Evaluate options and alternatives for E-Mail and select strategy.
 - a. Establish a temporary account for use while traveling. The Department of Administration’s Chief Information Officer (CIO) recommends using a temporary web based e-mail account in lieu the Wisconsin.Gov e-mail while traveling outside United States jurisdictions. Yahoo, G-Mail, Hotmail, etc. all provide a reasonable set of capabilities while traveling and then can be discontinued on return to the United States. The CIO also recommends limiting the number of e-mail contact and you should assume all communications are monitored. The following are questions and answers related to use of a temporary e-mail account.

 - b. Use of Outlook Web Access in lieu of, or in addition to, a Temporary E-Mail Account. This is not recommended; however, business needs may preclude the use of a temporary account.
 - Change Outlook Password
 - Obtain a sanitized loaner iPad or iPhone.
 - Configure for use with Outlook Web Access.
 - When checking e-mail disable Wi-Fi and connect to the web via 3G or 4G.

- [] 8. Review login credentials and passwords.
 - a. Do not use the same login credentials for state and personal business. For example a state ID Jon.Doe@wisconsin.gov should not use Jon.Doe as a user ID in other systems such as banking, on-line auctions, ext.

 - b. Do not repeat the same password for multiple applications. Where possible, ensure passwords for sensitive enterprise systems and do not use the same password for self-service passwords (e.g. email, calendar, etc.)

c. Make any necessary password changes warranted by this review, particularly for systems you will be accessing while abroad.

- [] 9. Encryption for e-mail. Recommend avoiding add-on encryption products to enable secure communications. Assume all communications are monitored. Encryption has both civilian and military purposes which are regulated by international law. **Rationale:** 1) Add-on encryption products may be intended for use in the United States and not appropriately licensed for foreign use. 2) Add-on encryption may give a sense of confidentiality that actually isn't present while traveling. 3) Encrypted traffic is easily detected that a foreign government may find suspicious and warranting further investigation.
- [] 10. Bluetooth. Recommend disabling all Bluetooth capabilities on Smart Phones, Tablets, Computers, audio devices, etc. Normally, this is a configuration setting and should be checked to insure it has not been accidentally enabled.
- [] 11. Familiarize yourself with local laws and security. Visit the U.S. State Department's web site to obtain information about the safety and security of the country you are visiting and to enroll in the Smart Traveler Enrollment Program (STEP).

DURING YOUR STAY:

- [] 1. Have no expectation of privacy. Eavesdropping is routine in some countries. Limit electronic and face-to-face discussion of sensitive information. If possible, wait to discuss sensitive matters upon return or using a known secure mechanism.
- [] 2. Treat electronic devices as compromised. Do not use computers or faxes at foreign hotels or business centers for sensitive matters. Do not allow foreign storage devices e.g. USB, CDs, etc. to be connected to your computer or phone. Do not connect your mobile device to a foreign computer for any reason (i.e. to sync data with your mobile device).
- [] 3. Keep electronic devices in your physical possession. Do not leave these devices unattended e.g. in your hotel room, in hotel safes, in your checked baggage, or do not ask someone to watch for you.
- [] 4. Only charge your device with the provided AC charger. Charging via a USB port on a foreign device provides a path to introduce malware.
- [] 5. Disable devices network capabilities when not in use. Turn off Bluetooth and Wifi capability on your device when you are not using. Consider turning off your cellular phone when it is not in use and particularly if you have a data plan enabled. This will conserve battery life and reduce the vulnerability to Wi-Fi or Bluetooth attacks.

- [] 6. Avoid installing software updates when using a hotel or other guest network. See FBI advisory “Travelers should avoid installing software updates when using a hotel or other guest network” available at: <http://www.ic3.gov/media/2012/120508.aspx>
- [] 7. Avoid accessing systems with sensitive or restricted information from abroad. This is particularly advisable in countries where there is no expectation of privacy. See the U.S. State Department's web site for country specific issues. In general, when accessing state systems minimize the length of time and amount of information accessed. Use VPN whenever possible to connect to state resources, unless you are in a country that doesn't allow or blocks encrypted data communications.
- [] 8. Immediately report loss or theft of information or electronic devices in accordance with the equipment provider's instructions.

UPON YOUR RETURN:

- [] 1. Clean and/or rebuild all electronic devices. Return the loaner equipment for analysis and cleaning. If you took your personal computer, we highly recommend that the laptop is analyzed for malware, unauthorized access and if necessary re-built before next use.
- [] 2. Change passwords. Consider changing passwords for all systems you accessed while traveling.


Statutory Authority

Wisconsin State Statute 16.97 (2)(a) provides that the department shall establish policies, procedures and planning processes for the administration of information technology services.

Human Resource Implications

In order to provide IT Risk Management, DET management shall:

1. Offer initial and continuing training to DET staff in IT Risk Management policy, processes, procedures and standards.
2. Ensure documentation for IT Risk Management policy, processes, and procedures documentation is accessible to all staff.
3. Ensure all DET staff consistently follows the IT Risk Management policy, processes, procedures, and standards.

	Chapter: Security
	Subject: International Travel Check List

DRAFT Published: August 10, 2016

4. Assist staff to understand IT Risk Management policy, processes, procedures, and standards, and enforce compliance with the policy, processes, procedures, and standards.

Related Policies, Processes, Procedures, Standards, or Best Practices

The Federal Bureau of Investigation: Safety and Security for the Business Professional Traveling Abroad. Available at:

<http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure>

DET Acceptable Use

DET Asset Management & Classification

DET Asset Protection

DET Wisconsin Configuration & Asset Management

DET Incident Management

DET Security Staff

DET Threat Assessment & Monitoring

DET Vulnerability Assessment & Risk Management

System and Application SOPs

NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems"

NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems"

Additional Information

E-MAIL COMMUNICATIONS

When traveling internationally a temporary e-mail account that is only active during the international travel period will limit personal and professional exposure both during and after the travel.

Travelers should assume that all overseas telecommunications can be intercepted, recorded, organized into reports, and reviewed for intelligence purposes. Employees should be aware of the following:

1. Intelligence agencies of third-party nations, terrorists, and criminals monitor electronic transmissions;
2. Government, business, and technical data obtained from U.S. citizens may be, and often are, provided to terrorists; and

3. Personal information obtained may be used for financial gain, political, or other malicious purposes.

The following are Q&As concerning temporary accounts.

1. **Why use a temporary account?** Foreign actors are motivated by a number of factors and represent a real and significant threat to travelers from the United States. The objective of the temporary account is to minimize your digital foot print to avoid becoming a target or facilitating the targeting of others.
2. **Why limit e-mail contacts?** By maintaining only a limited number of contacts, also via temporary accounts, you will establish a digital boundary that will minimize your exposure both during and after the international travel. See Appendix 1.
3. **Should I auto forward my Wisconsin.Gov e-mail?** No. This defeats the purpose of using a temporary account to limit communications. Also, the temporary account is most effective when only known by a few individuals. This means the temporary account should not be used in out of office messages.
4. **If this is more secure, why not at home?** In the United States every day millions of trusted connections are established between remote devices and organizational servers. So at home one connection to a State of Wisconsin server is one of millions. When traveling abroad a connection from a remote device to a State of Wisconsin server is easily identified on foreign networks and available for foreign analysis. Encryption and virtual private networks offer some protection; however, network traffic can be archived and days or weeks devoted to unencrypting the traffic. By using temporary accounts you reduce the possibility of your digital identify being used for nefarious purposes during or after travel.
5. **What about Open Records?** In general it is important to determine the individual agency's record retention policies as it applies to records created in the course of international travel. In general it is important to realize in any context it is the content of the record, not the medium that determines if the record is subject to the state's laws on public records retention and disclosure. Upon return to the United States, any business related communications on a temporary web based email account should be printed and appropriately retained. Do not forward them to your Wisconsin.gov email account. After all public records have been printed; please deactivate the web based email account.
6. **Our Agency has a Virtual Private Network (VPN) isn't that secure?** No. Even virtual private network technology is susceptible to risks such as:


- Lack of required host security software on public machines
 - Physical access to shared machines
 - Keystroke loggers
 - Endpoints—loss of sensitive information and intellectual property
 - Man-in-the-middle attacks
 - Hardware limitation
7. **What about digital pictures?** There are several sources of photographic material.
- If a camera is used a new flash memory card should be dedicated to the travel and carefully analyzed on return.
 - Photo sharing services such as www.flickr.com; www.shutterfly.com; or www.photobucket.com provide a mechanism to upload directly from a mobile device.
 - Smart phone photos can safely be sent via e-mail, provided the receiving computer has up-to-date antivirus protection.

BLUETOOTH

Bluetooth should be turned off to avoid numerous international Bluetooth exploits.

Bluetooth is a wireless networking technology that allows a wide range of devices to communicate wirelessly through automatic connections. Because it uses radio technology, generally a 32 foot radius, it is susceptible to eavesdropping and may provide hackers with access to Bluetooth enabled devices. The following are common terms associate with Bluetooth exploits.

1. Bluejacking. A hacker sends a v-card to the target Bluetooth user. If the user allows the contact to be added to his address book, and the contact can send him messages may be automatically opened because they're coming from a known contact
2. Bluebugging. Allows hackers to remotely access a user's phone and use its features, including placing calls and sending text messages without the users knowledge.

	Chapter: Security
	Subject: International Travel Check List

DRAFT Published: August 10, 2016

3. Car Whisperer. This is software that allows hackers to send audio to and receive audio from a Bluetooth-enabled car stereo.

If the event Bluetooth capabilities are a business necessity it should be enabled only when required and enabled in hidden or non-discoverable mode. Otherwise Bluetooth should always be disabled.

ENCRYPTION

Today virtually every consumer device or computer has some inherent or supplemental encryption technology. These technologies generally do not pose a problem; however, there may be restrictions on the use of encryption during international travel. The following are useful links:

1. Special provision: restrictions for export or re-export of technology. See: <http://www.gpo.gov/fdsys/pkg/CFR-2012-title15-vol2/pdf/CFR-2012-title15-vol2-sec740-14.pdf>
2. Dual-Use List – Category 5 – Part 2 – Information Security. See: <http://www.wassenaar.org>

LAPTOP COMPUTER PREPARATIONS

State of Wisconsin employees are encouraged not to bring a laptop overseas unless there is a compelling reason to do so. If a laptop is needed they should request a loaner laptop if time permits. The traveler should only load the files they need overseas to minimize potential loss of data. All laptops taken overseas shall adhere to the following:

1. Protected by a full-disk encryption technology solution;
2. All wireless capabilities, including but not limited to Wi-Fi, Bluetooth, and broadband cards, shall be disabled;
3. Device shall remain under the direct and immediate control of the employee or authorized government contractor); and
4. Any laptop used in overseas shall not be reconnected to State of Wisconsin systems or networks until sanitized.

Notebook Hard Drive Preparation Before and After.

Sanitizing the computer means wiping all data and programs from the computer hard drive. To avoid loss of data the traveler should back up their files prior to travel. Laptop computer hard drives may return infected with malware. IT Staff have a variety of tools,

techniques, and procedures to permanently remove information prior to travel and sanitize the drive on return.

Before:

Hard drives and solid-state drives (SSDs) retain their data even if the files are deleted, thus can be recovered using software or magnetic recovery techniques, but only hard drives can be easily scrubbed with a disk utility. When sanitizing a drive for travel:

WINDOWS: IT staff should utilize windows utility, www.fileshreder.org, to permanently delete files and remnants of files.

APPLE: Place files in the Trash can and use the Finder > Secure Empty Trash option. Then to insure remnants of previously deleted files are erased Open Disk Utility and click on the partition you want on the left then Erase and Erase Free Space > Zero (long, good enough) or 7x (longer, stronger).

Appendix 1: Sanitizing Devices for the IT Professional.

The following information is provided for agency IT professionals responsible for the sanitation of notebook computers used in international travel.

DET does not have a specific workstation disposal policy or standard for the sanitation of notebook computers. Internally, DET follows the NIST SP 800-88 Guidelines for Media Sanitization (Sept. 6, 2012). See: <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-88-Rev.%201>.

DET does not specifically endorse or recommend a specific product. The following products are available as of October 16, 2013.

Product Name: OnTrackEraser
ONTRACK Data International, Inc.
9023 Columbine Road, Eden Prairie, MN 55347
Toll Free: 1 (800) 872-2599
[http:// www.ontrack.com](http://www.ontrack.com)

Product Name: CyberScrub Security w/ Media Wiper"
CyberScrub Corporation
Sales: (770) 951-2080
[http:// www.cyberscrub.com](http://www.cyberscrub.com)

Product Name: Easy File Shredder
WebMinds
support@webminds.com
8540 Dayton Avenue
Fort Myers, FL, USA
33907
<http://www.easyfileshredder.com/>

Product: WipeDrive SystemSaver
White Canyon Software
947 South 500 East, Suite 300
American Fork, UT, USA 84003
Sales: 1 (801) 224-8900
WebSales@WhiteCanyon.com
<http://www.whitecanyon.com/>

Product: Drive eRazer™ Ultra
WiebeTech
8201 E. 34th Circle N., Suite 909
Wichita KS, 67226
Sales@wiebetech.com
Sales: 866-744-8722
http://www.wiebetech.com/products/Drive_eRazer_Ultra.php

Appendix 2: Outlook Web Access Illustration

Q: Why waste the time and effort to use a temporary account? Doesn't the padlock image mean my information is encrypted?

A: No. There are two major vulnerabilities packet capture by anyone with access to the network and the possibility of a key logger secretly installed on your computer or smart phone. If OWA is used 3G/4G connections provided an extra layer of security.

Key Loggers:

The availability of Key Loggers (e.g. Keyloggers.com) is the biggest reason to not use Out Look Web Access (OWA). If your system is compromised as soon as you log into OWA, then anyone else can login to OWA and access your work E-mail account. This is part of the justification for a temporary external E-mail account while traveling internationally. The temporary account prevents evil doers from:

- 1) Logging on to your State of Wisconsin E-mail and viewing ALL of your E-mail, calendar and contacts. Whereas with a temporary account if your computer is compromised the evil doer only has access to e-mail in that account.
- 2) Using your State of Wisconsin E-mail to send counterfeit messages apparently from you. This could be a phishing message that your contacts are likely to click on since it came from a State Of Wisconsin account.
- 3) Attempting to access other systems where same or similar E-mail usernames and passwords have been used. In short an evil doer with access to one compromised system will attempt to guess their way into accounts on other systems (such as Ebay, linked-in, Facebook, banks, etc.)

1 - Infiltration	Reconnaissance	Actors search open sources to identify and assess targets for collection and entities/relationships to exploit in the attack.
	Infection	Typically, well-crafted spear phishing e-mails with linked or embedded files containing malicious code serve as the intrusion vector.
2 - Persistence	Establish Backdoors	Attackers maintain network footholds by obtaining domain administrative credentials and moving laterally through a network, establishing multiple backdoors.
	Enumerate the Network	Persistent threat intruders laterally enumerate a network gathering valid credentials (user accounts and passwords) for multiple systems.
	Install Utilities	Attackers install any number of several malicious utilities necessary to maintain persistence and ultimately steal information.
3 - Exfiltration	Escalate Privileges	With access and persistence established, intruders escalate their privileges and prepare for exfiltration.
	Harvest Data	Specific documents and e-mails containing targeted data are collected and packaged into a single, encrypted, and password-protected compressed file.
	Exfiltration	The intruders exfiltrate the compressed file to another compromised system in their command and control infrastructure.
	Conceal Activity	Finally, intruders either attempt to clean up their tools, maintaining persistence, or set the attack in a dormant state to evade detection while maintaining access.

Packet Capture:

Network monitoring software is capable of capturing and decoding packets of data. 3G/4G network connections increase the level of sophistication and access required to capture packets.


The following illustrates the information that can be obtained from public WI-FI or hotel / business center “secured” network connection. This illustrates one packet in a normal logon prior to establishing the secure link. In the address <http://mail.wisconsin.gov> was entered. The packet reveals:

- 1) Location of the employee logging on the Wisconsin.Gov via IP address. This can be used for a number of nefarious purposes.
- 2) The fact that Wisconsin.Gov hosts Outlook Web Access (OWA). OWA vulnerabilities can be found on support.microsoft.com.
- 3) The client computer is running Internet Explorer (IE) 8.0 – an out of date browser. IE vulnerabilities can be found on support.microsoft.com.
- 4) Cookies are enabled.
- 5) The server is ?BIGipServer~PROD_MAIL~POOL_MAIL?

```

0000 47 45 54 20 2f 6f 77 61 2f 61 75 74 68 2f 6c 6f GET /owa/auth/lo
0010 67 6f 6e 2e 61 73 70 78 3f 75 72 6c 3d 68 74 74 gon.aspx?url=htt
0020 70 3a 2f 2f 6d 61 69 6c 2e 77 69 73 63 6f 6e 73 p://mail.wiscons
0030 69 6e 2e 67 6f 76 2f 6f 77 61 2f 26 72 65 61 73 in.gov/owa/&reas
0040 6f 6e 3d 30 20 48 54 54 50 2f 31 2e 31 0d 0a 41 on=0 HTTP/1.1..A
0050 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 ccept: /*/*..Acce
0060 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encoding: gzi
0070 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 p, deflate..User
0080 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0090 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 4.0 (compatible;
00a0 20 4d 53 49 45 20 38 2e 30 3b 20 57 69 6e 64 6f MSIE 8.0; Windo
00b0 77 73 20 4e 54 20 36 2e 31 3b 20 54 72 69 64 65 ws NT 6.1; Tride
00c0 6e 74 2f 34 2e 30 3b 20 53 4c 43 43 32 3b 20 2e nt/4.0; SLCC2; .
00d0 4e 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 NET CLR 2.0.5072
00e0 37 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 7; .NET CLR 3.5.
00f0 33 30 37 32 39 3b 20 2e 4e 45 54 20 43 4c 52 20 30729; .NET CLR
0100 33 2e 30 2e 33 30 37 32 39 3b 20 4d 65 64 69 61 3.0.30729; Media
0110 20 43 65 6e 74 65 72 20 50 43 20 36 2e 30 3b 20 Center PC 6.0;
0120 2e 4e 45 54 34 2e 30 43 3b 20 2e 4e 45 54 34 2e .NET4.0C; .NET4.
0130 30 45 3b 20 2e 4e 45 54 20 43 4c 52 20 31 2e 31 0E; .NET CLR 1.1
0140 2e 34 33 32 32 3b 20 49 6e 66 6f 50 61 74 68 2e .4322; InfoPath.
0150 33 29 0d 0a 48 6f 73 74 3a 20 6d 61 69 6c 2e 77 3)..Host: mail.w
0160 69 73 63 6f 6e 73 69 6e 2e 67 6f 76 0d 0a 43 6f isconsin.gov..Co
0170 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 nnection: Keep-A
0180 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 63 6f live..Cookie: co
0190 6f 6b 69 65 54 65 73 74 3d 31 3b 20 42 49 47 69 okieTest=1; BIGI
01a0 70 53 65 72 76 65 72 7e 50 52 4f 44 5f 4d 41 49 pServer~PROD_MAI
01b0 4c 7e 50 4f 4f 4c 5f 4d 41 49 4c 3d 31 35 32 35 L~POOL_MAIL=1525
01c0 38 35 32 32 36 2e 32 30 34 38 30 2e 30 30 30 85226.20480.0000
01d0 3b 20 61 76 72 5f 33 30 37 35 37 33 38 36 39 33 ; avr_3075738693
01e0 5f 30 5f 30 5f 34 32 39 34 39 30 31 37 36 30 5f _0_0_4294901760_
01f0 37 34 34 32 37 35 33 36 35 5f 30 3d 31 38 39 33 744275365_0=1893

```

	Chapter: Security
	Subject: International Travel Check List <p style="text-align: right;">DRAFT Published: August 10, 2016</p>

0200 38 39 39 30 36 37 5f 31 36 36 31 37 30 33 31 0d 899067_16617031.
 0210 0a 0d 0a ...

While the information gained may seem unimportant when combined with other sources of information related to the State of Wisconsin Infrastructure provides an evil doer or nation state actor with information required to launch a significant attack.

Appendix 3: Virtual Private Networks

Virtual Private Networks (VPN).

The State of Wisconsin VPN allows employees to securely access the State's network while traveling in the United States and may work in other countries. However, several countries employ a national strategy for web filtering which may block VPN connections. . Because DOA/DET does not have the global presence to manage an international VPN architecture the State of Wisconsin VPN software should be removed from notebook computers used in international travel.

When traveling in a country where the infrastructure may be in question VPN security can be compromised by either a key logger or man-in-the-middle interception of VPN traffic. If a VPN user is IT savvy and knows which VPN certificate they are using then it is possible to detect the changed certificate then man-in-the-middle can be detected. Most business travelers won't conduct this type of analysis.

Internet filtering and interception is not unique to State of Wisconsin travelers. DET does not recommend the use of a private paid VPN to circumvent a government's filtering of internet traffic. Free VPN services are easily blocked by whoever is enforcing the filtering policy. The following products are available as of October 16, 2013.

1. 12VPN. <https://12vpn.com>
2. StrongVPN. <http://strongvpn.com>
3. ConnectionVPN. <https://connectionvpn.com>

This is not a tacit endorsement to use a paid VPN; however, these sites can provide more detailed information concerning VPN Services.