2022
TRADE FACILITATION AND CARGO SECURITY SUMMIT
Hosted By: U.S. Customs and Border Protection

CTPAT Workshops:
Minimum Security Criteria (MSC) Update with a focus on Cybersecurity and Agriculture

2022
TRADE FACILITATION AND CARGO SECURITY SUMMIT
Hosted By: U.S. Customs and Border Protection

MSC Update- Agricultural Security
Stephanie Lee
July 20, 2022

Agricultural Security

Agriculture is the largest business sector

↓

Contaminants are found in all types of transportation (352 pests discovered daily by CBP)

↓

Pollutants harbor pests and diseases

↓

Threaten the agro-industry

↓

We know it … and so do the terrorists

↓

Objective - Destroy our Economic Viability

Agricultural Security

MSC Section 8: Agriculture Security

- CTPAT members MUST have **written procedures** designed to prevent visible pest contamination, including compliance with Wood Packaging Materials (WPM) regulations.
- The Measures Concerning **Wood Packaging Materials** MUST comply with the International Plant Protection Convention (IPPC)'s International Standards for Phytosanitary Measures No. 15 (ISPM 15).
- Measures to **prevent visible pests** must be adopted throughout the supply chain.

Agricultural Security

Definition of Pest Contamination - International Maritime Organization

Pest contamination is defined as **visible** animals, insects or other invertebrates (alive or dead, at any stage of the biological cycle, including egg shells) or any organic or animal material (including blood, bones, hair, tissue, secretions, excretions); viable or non-viable plants or plant products (including fruits, seeds, leaves, branches, root, bark); or other organic material, including fungi; or soil, or water; where such products are not part of the manifested cargo within international traffic instruments (e.g., containers, unit load devices, etc.)

Visible = Specialized equipment not required to perform the inspection.

Agricultural Security

Definition of Wood Packaging Materials:

Wood or wood products (excluding paper products) used to hold, protect or transport a product (including dunnage).

Agricultural Security

Examples of wooden packaging materials:

Bars
Boxes
Crates
Containers
Reels

Wooden Crates

Cages Brackets
Planks Drums
Pallets

Agricultural Security

Wooden packaging material does not include:

- ✓ Packaging made entirely of thin wood (6mm thick or less).
- ✓ Packaging made entirely of processed wood material, such as plywood, particle board, oriented strand board, or veneer sheets that have been created using glue, heat or pressure, or a combination thereof.
- ✓ Sawdust, shavings and wood wool

Agricultural Security

Wood Packaging Materials- IPPC - ISPM 15 (NIMF 15) and 7 CFR 319.40

Meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No.15 (ISPM 15) .

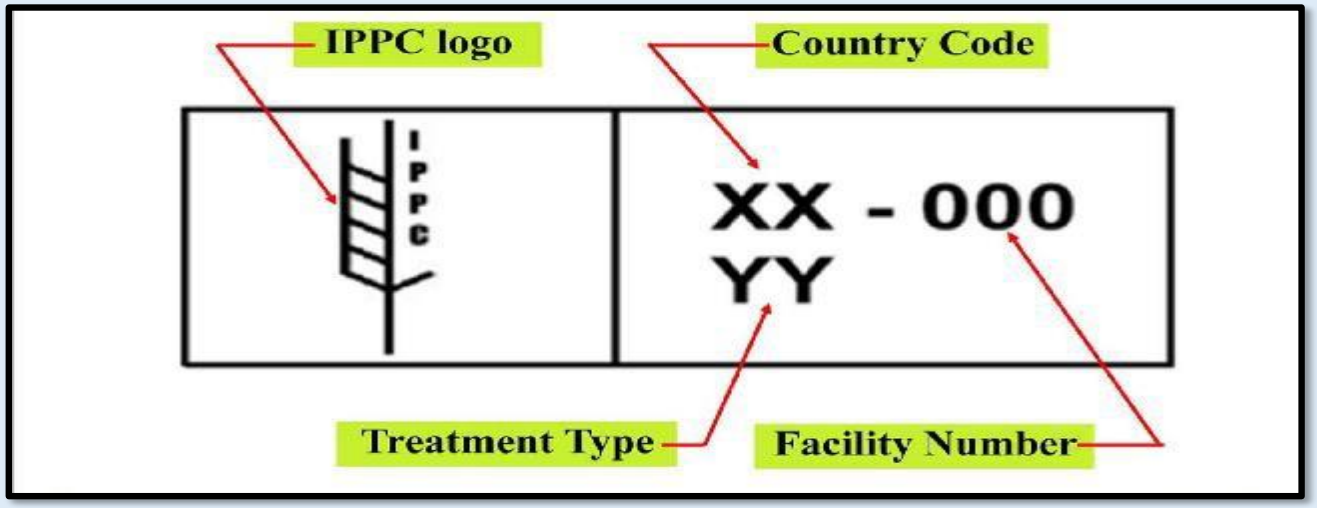
IPPC - Treaty under the supervision of the United Nations' Food and Agriculture Organization

ISPM 15 - Internationally-accepted measures which require that:

- ✓ WPM is debarked and subsequently heat-treated or fumigated with methyl bromide;
- ✓ Stamped or branded with the IPPC mark of compliance ("wheat stamp")

Agricultural Security

International Plant Protection Convention (IPPC) Logo

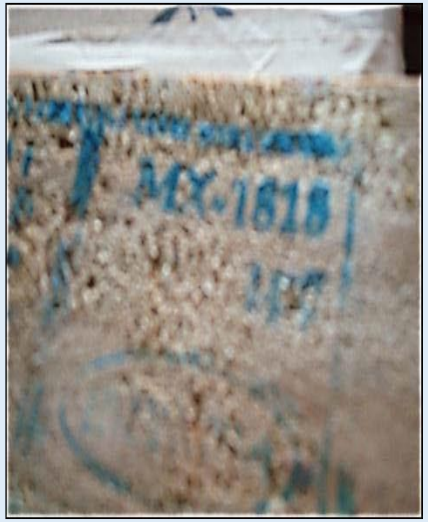


Each unit of WPM must be marked

Agricultural Security

Correct Logo

Agricultural Security




WPM Marked Inappropriately

Agricultural Security

Consequences for Non-compliance

- Load will be **re-exported**
- Load may be **fumigated** by USDA prior to re-export

Agricultural Security

What can you do to comply with the standard?

- Make sure your wood packaging materials supplier is accredited (ISPM 15).
- Educate your supply chain on the requirements of ISPM 15
- Find alternatives to WPM - Cost Benefit Analysis

Agricultural Security

MSC Section 5: Transportation and Instruments of International Traffic (IIT) Security

5.2 - The inspection process must have **written procedures** focused on **agricultural inspections.**

5.3 - **Before loading**, you must carry out agricultural and safety inspections

5.7 - If contamination is found, clean the IIT / SIN = Secure, Isolate, Notify

5.9 - AGM Pre-Departure Certificates (Ocean Carriers Only)

5.10 - Agricultural and safety inspections for Air Carriers

Agricultural Security

5.3 - Perform an Agricultural inspection in accordance with CTPAT on Instruments of International Traffic (IIT)/ Transport

Ensure that transportation is clean before loading the goods

Keep vegetation near the facilities cut down, as these areas can harbor insects and rodents.

Sweep, vacuum, wash, steam and/or pressure wash the Instruments of International Traffic (containers, "cookie sheets," trailers, etc.) before loading merchandise

Avoid loading when insects swarm

Vacuum seeds from the Wooden packaging Materials

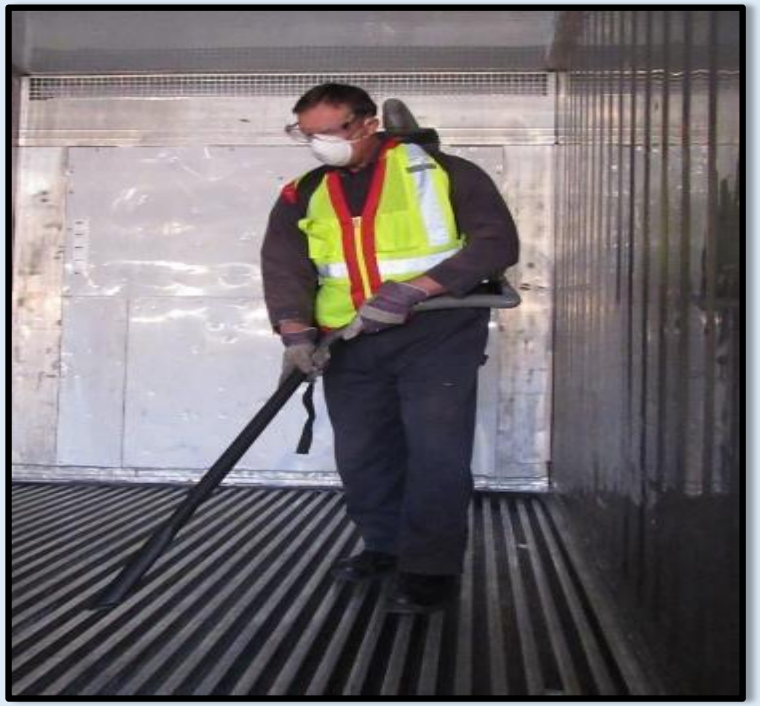
Properly store and cover Instruments of International Traffic (platforms, bars, crates, etc.)

Spray contaminated Instruments of International Traffic

Park trailers away from green areas and/or avoid placing them on the ground or on vegetation.

Bright lights attract insects, especially at night. Keep container doors closed while the merchandise is not being loaded

Agricultural Security



Eliminating Contaminants - Vacuum, Broom, Blower

Agricultural Security

Start with a Clean Container Before Loading

Use Paved Lots to Avoid Contamination

2022 TRADE FACILITATION AND CARGO SECURITY SUMMIT

Hosted By: U.S. Customs and Border Protection

Agricultural Security

MSC Section 7: Procedural Security

7.2 - Loading areas must be inspected - Free from contamination by pests

7.11 - Trash must be stored and disposed of properly - Only for Ocean Carriers

7.12 - Driver must discard or declare personal garbage - Highway / Crossing Carriers; 3PLS

MSC Section 12: Education, Training and Awareness

12.2 - Agricultural Inspection Training

12.7 - Agricultural Contaminant Prevention Training

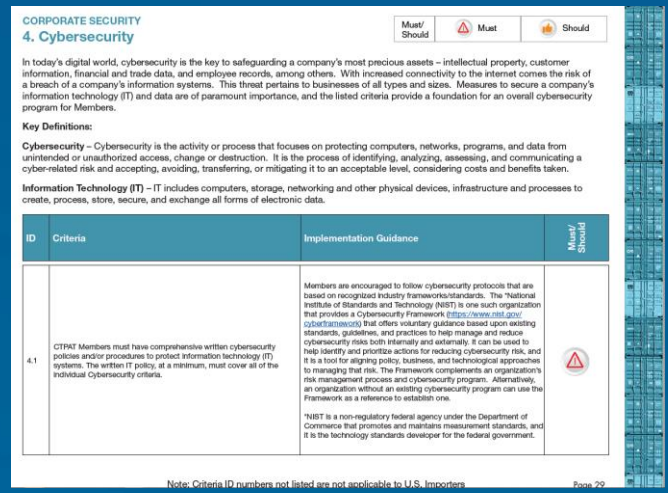
Agricultural Security

2022
TRADE FACILITATION AND CARGO SECURITY SUMMIT
Hosted By: U.S. Customs and Border Protection

MSC Update- Cybersecurity
Bryan Smith
July 20, 2022

June 2020 – New MSC Released

- Significant enhancement to cybersecurity MSC
- In-line with government and industry norms
- New MSC developed with significant input from CTPAT members



CORPORATE SECURITY

4. Cybersecurity

Must/Should | Must | Should

In today's digital world, cybersecurity is the key to safeguarding a company's most precious assets – intellectual property, customer information, financial and trade data, and employee records, among others. With increased connectivity to the internet comes the risk of a breach of a company's information systems. This threat pertains to businesses of all types and sizes. Measures to secure a company's information technology (IT) and data are of paramount importance, and the listed criteria provide a foundation for an overall cybersecurity program for Members.

Key Definitions:

Cybersecurity – Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change or destruction. It is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken.

Information Technology (IT) – IT includes computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.

ID	Criteria	Implementation Guidance	Must/Should
4.1	CTPAT Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.	Members are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/standards. The "National Institute of Standards and Technology (NIST) is one such organization that provides a Cybersecurity Framework (https://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines, and practices to help manage and reduce cybersecurity risks both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The Framework complements an organization's risk management process and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. *NIST is a non-regulatory federal agency under the Department of Commerce that promotes and maintains measurement standards, and it is the technology standards developer for the federal government.	⚠

Note: Criteria ID numbers not listed are not applicable to U.S. Importers

Page 29

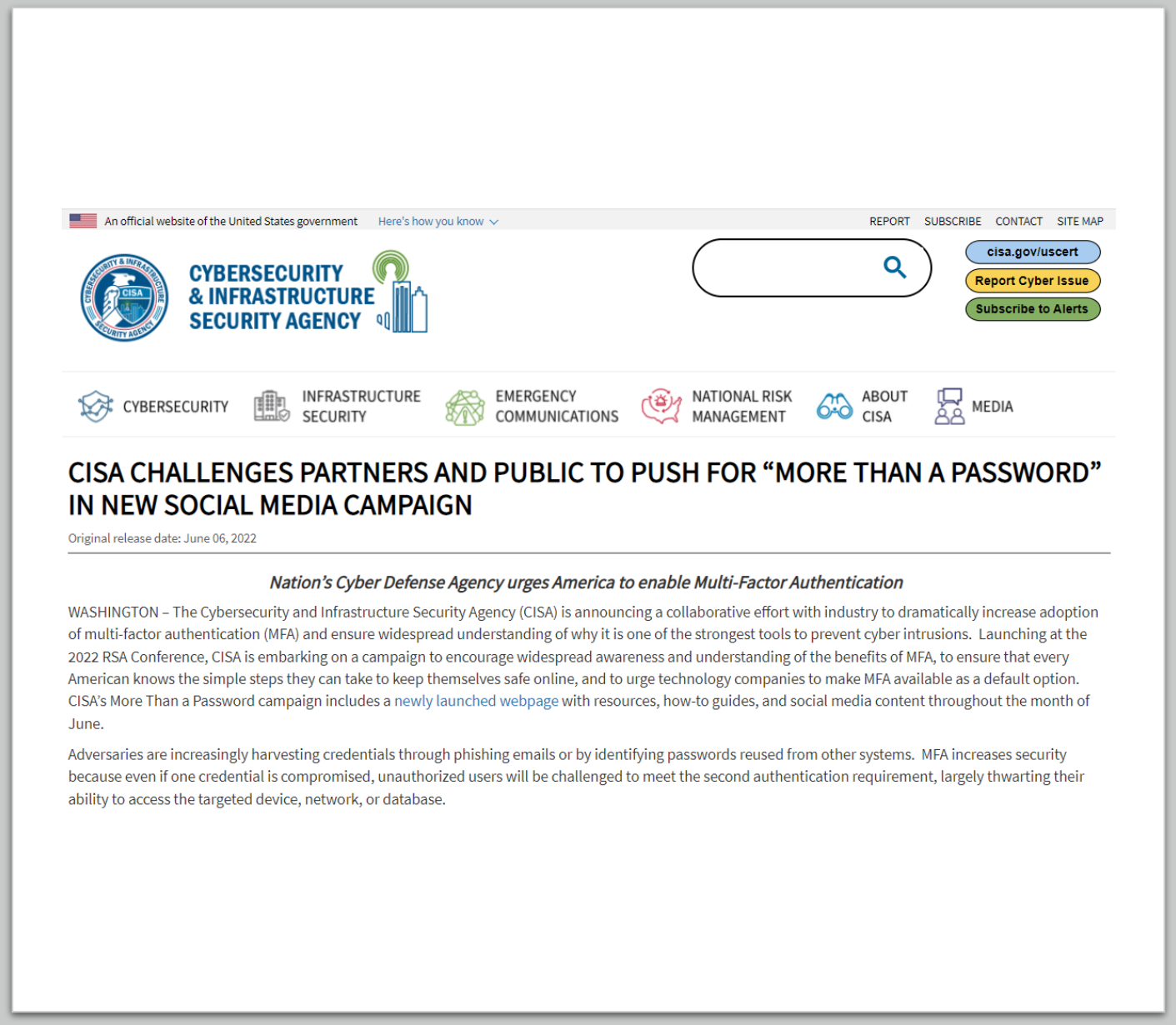
Whereas CTPAT is just one component out of several that were created by Commissioner Bonner in the wake of the 9/11 attacks to create a layered approach to homeland security and extend our borders, the same approach should be taken when implementing this program. There is a layered approach to cybersecurity

June 2020 – New MSC Released

- All CTPAT Field Offices held new MSC workshops prior to launch in 2019, early 2020
- Videos published on CBP's YouTube channel
- 'Layered' defense strategy – all MSC are critical
- CTPAT members required to ensure foreign partners are compliant with MSC – this includes cybersecurity!

July 2022

- All sources indicate cyber threat persists
- Threat actors are spending more time ‘hands-on’
- FBI/NSA/NIST are still instructing private industry to adopt many of the procedures found in the CTPAT cyber MSC
- The CTPAT MSC forces companies to take a hard, in-depth look at their internal operations



An official website of the United States government Here's how you know

REPORT SUBSCRIBE CONTACT SITE MAP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

CISA CHALLENGES PARTNERS AND PUBLIC TO PUSH FOR “MORE THAN A PASSWORD” IN NEW SOCIAL MEDIA CAMPAIGN

Original release date: June 06, 2022

Nation’s Cyber Defense Agency urges America to enable Multi-Factor Authentication

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) is announcing a collaborative effort with industry to dramatically increase adoption of multi-factor authentication (MFA) and ensure widespread understanding of why it is one of the strongest tools to prevent cyber intrusions. Launching at the 2022 RSA Conference, CISA is embarking on a campaign to encourage widespread awareness and understanding of the benefits of MFA, to ensure that every American knows the simple steps they can take to keep themselves safe online, and to urge technology companies to make MFA available as a default option. CISA’s More Than a Password campaign includes a newly launched webpage with resources, how-to guides, and social media content throughout the month of June.

Adversaries are increasingly harvesting credentials through phishing emails or by identifying passwords reused from other systems. MFA increases security because even if one credential is compromised, unauthorized users will be challenged to meet the second authentication requirement, largely thwarting their ability to access the targeted device, network, or database.

Metrics – Since June 2020

- MSC 4.1 Comprehensive cybersecurity policies
- MSC 4.8 User Authentication/MFA/VPN
- MSC 4.4 Sharing Information with partners/government

IT Department – Full Inclusion

- **There should be no gap between the implementation of physical security controls and cybersecurity controls.** All CTAPT MSC are created equal. Just as CTPAT requires partners to start with a risk assessment the same principle should be applied in assessing their degree of risk associated with the network security of their organization. Then, this should be expanded to include assessing their business partners as risks associated with supply chain attacks is on the rise.

Risk Based Approach

Analyze current level of compliance with IT norms and the CTPAT Cyber MSC

Engage

IT should be allowed to speak freely about weaknesses, and possible solutions needed to mitigate vulnerabilities

IT Department Engagement

Assessing partners for IT security
Including IT department in assessing partner and the onboarding process.

Top Level Considerations

Lack of Oversight
The IT department has little to no real oversight. Overburdened, lack of experience

Discussions
Discussions with IT department need to include senior managers. Those discussions must have value and be acted upon

Security Teams
IT department must be included in security teams and meetings

Managerial Involvement
Not to serve as a figurehead but have an active role and provide updates to the senior leadership with meaningful metrics and deliverables.

Comprehensive Cybersecurity Policies
For staff members, but also enterprise-wide considerations and for the IT department specifically.

Cybersecurity Policies – Audit/Oversight
Policies should be written in a manner that will give managers a tool for maintaining oversight and conducting audits

Crisis Response – Recovery Plan
Formal plan to respond to disaster, cyber incident. Rehearsed, conduct drills, tests

External Help
Managers may want to consider independent, third-party audit and assistance (MSP)

MSC 4.1 Comprehensive Policy

- Comprehensive policies are the backbone of a successful cybersecurity program
- Staff, acceptable use, rules, etc.
- IT Staff or Third Party managed service provider (MSP) – Inclusive security team, increased comms
- Tools for oversight, auditing and generate evidence of implementation for validation

CTPAT Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.

MSC 4.1 Comprehensive Policy

- Discuss with IT staff. Require they demonstrate how each criterion is covered in policy and that they are adhering to policy and the MSC.
- Use policy as a guide during audits.
- Review policy regularly as a team, after-action reviews.
- "…At a minimum, policies must cover all of the individual cybersecurity criteria."

MSC 4.1 Comprehensive Policy

- Crisis management/business resumption –
  - Allow IT make time sensitive decisions (MSC 2.4)

- IT Department (or MSP) policies – Internal requirements for IT

MSC 4.8 User Authentication

- Strong passwords – not enough anymore, lack of training, shortcuts
- Multi-factor authentication (MFA)
- Require MFA for all sign-ons, web-based email.
- www.cisa.gov/mfa - CISA's MFA Page

MSC 4.4 Sharing

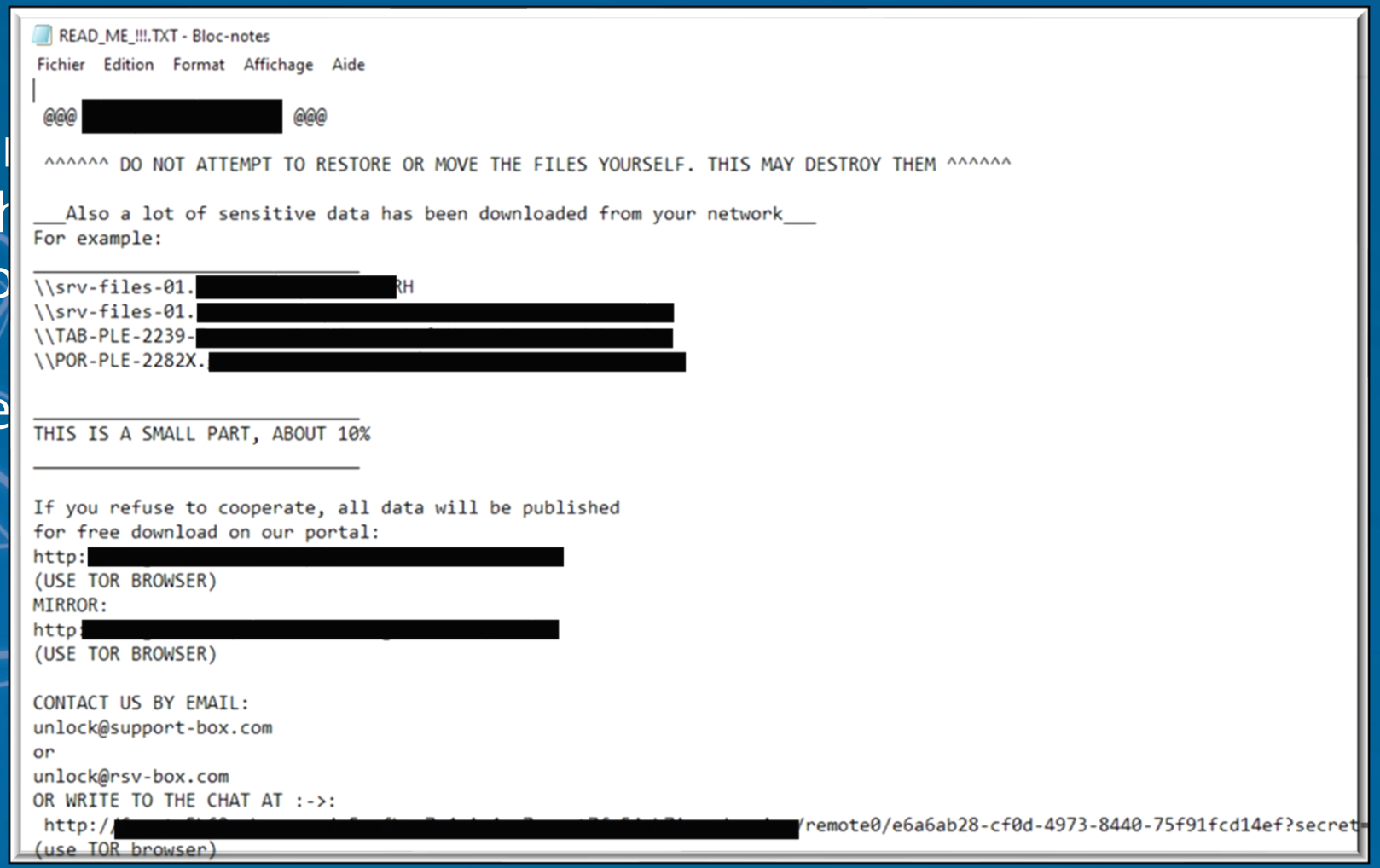
- Members are strongly encouraged to share information with business partners, government
- Indicators of compromise
- Should consider sharing threat information with your business partners
- Notifying government agencies could help protect spread of threats. Benefits of working w/ LE are evident to CTPAT
- Incorporate into policy, retain EOI for validation

MSC 4.2

- Patches-Security Updates
- Not in policy, no formal requirements
- CISA - malicious cyber actors continued to exploit publicly known, dated software vulnerabilities—some of which were also routinely exploited in 2020 or earlier. The exploitation of older vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.
- End of Life

Breach

- Malware may lay do
- Triggered Friday nigh
- Actors spend time lo
  navigate laterally
- Launch ransomware
- Instructions may be



READ_ME_!!!.TXT - Bloc-notes

Fichier Edition Format Affichage Aide

@@@ [redacted] @@@

^^^^^^ DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM ^^^^^^

___Also a lot of sensitive data has been downloaded from your network___

For example:

_____

\\srv-files-01.[redacted]RH

\\srv-files-01.[redacted]

\\TAB-PLE-2239-[redacted]

\\POR-PLE-2282X.[redacted]

_____

THIS IS A SMALL PART, ABOUT 10%

_____

If you refuse to cooperate, all data will be published
for free download on our portal:

http:[redacted]

(USE TOR BROWSER)

MIRROR:

http[redacted]

(USE TOR BROWSER)

CONTACT US BY EMAIL:

unlock@support-box.com

or

unlock@rsv-box.com

OR WRITE TO THE CHAT AT :->:

http:/[redacted]/remote0/e6a6ab28-cf0d-4973-8440-75f91fcd14ef?secret=

(use TOR browser)

Breach

- Lack of comprehensive cybersecurity policies for employees *and* IT personnel (MSC 4.1)
- IT department had little to no oversight by knowledgeable persons
- Company lacked a formal and documented business resumption plan (MSC 4.2)
- Did not store backups appropriately (no segregation)
- Offered little to no cybersecurity training to employees (MSC 12.8)
- Patch management was questionable and had flaws (MSC 4.2)
- Network was not mapped (MSC 4.2)
- VPN deployed without 2FA enabled
- Lack of network segmentation – possibly allowing lateral movement

Here are the communications.

Hello - You have attacked us and encrypted our files and we would like to discuss your demands in order to get decrypor and assurance you will delete our files.

[redacted] 4:52:34 PM
hi •

[redacted] 5:01:27 PM
we have 250gb of your data and your systems are locked. even if you use backups, and if we cannot get agreement we will post your data about employees clients cont and provide as proof. our demand are 1.5kk to close this problem. we will provide decryptor and delete your files from our storage. we advise quick decision •

[redacted] 5:36:17 PM

Could you decrypt the files I uploaded and can you provide us with a list of file you took?

[redacted] 5:37:44 PM
our internal process will not agree to give filetree until you pay and then we can give. the ransom note has some sample of places we take data •

[redacted] 5:42:34 PM

Breach

- Supply Chain integrity is compromised
  - Virtual
  - Physical
- Degradation in business operations
- Loss of proprietary/customer information
  - Published on the web
- PII exploitation
- Fines, penalties
- Loss of business, revenue
- Costs associated with a ransomware attack

Questions?

Stephanie Lee
Supply Chain Security Specialist
562-366-3273
Stephanie.s.lee@cbp.dhs.gov

Bryan Smith
Supply Chain Security Specialist
201-286-0920
Bryan.d.smith@cbp.dhs.gov

Adam Gunion
Supervisory Supply Chain Security Specialist
562-366-3878
Adam.t.gunion@cbp.dhs.gov