NELLIS AFB
NETWORK INCIDENT REPORTING CARD

** Current as of 10/3/2023 **

OPSEC – DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS

COMPUTER VIRUS
REPORTING PROCEDURES FOR USERS

STEP 1	**STOP! DISCONNECT THE NETWORK CABLE.** *Discontinue Use*
STEP 2	**LEAVE THE SYSTEM POWERED UP.** Personnel *WILL NOT* click on any prompts, close any windows, or shut down the system.
STEP 3	If a message appears on the monitor of the affected system, ***WRITE IT DOWN!***
STEP 4	**WRITE DOWN ALL ACTIONS** that occurred during the suspected virus attack, e.g., received suspicious e-mail with attachments, clicked a link, inserted a disk, plugged in a USB device, downloaded a file, etc.
STEP 5	**REPORT IT IMMEDIATELY!** Contact your unit Cybersecurity Liaison (CL), Unit Security Manager (USM), or Commander's Support Staff (CSS). The Nellis Communications Focal Point (CFP) may be contacted if your CL/USM/CSS are not available. **DSN 652-2666, Opt 1 for Nellis.**

NOTE: When reporting a suspected virus to your CL, CSS, or CFP, ensure you give the following information to the technician:

- Event date and time
- Your name and telephone number
- Building and room number
- Name of anyone who has assisted you
- Location of infected system

NEGLIGENT DISCHARGE OF CLASSIFIED INFORMATION (NDCI)
REPORTING PROCEDURES FOR USERS

An **NDCI** occurs when classified information is transferred onto an unclassified information system, e.g., sent email, received email, created a document, scanned/copied on a NIPR printer/copier, etc.

STEP 1	**STOP! DISCONNECT THE LAN CABLE**: safely pull out the ethernet cable connecting the affected computer(s) or printer to the network. **DO NOT POWER OFF!** If affected device (sending or receiving) is a mobile device: ****IMMEDIATELY** contact CFP to disable BUEM App FIRST.** Once disabled, sanitize the phone. Your CL can sanitize – if not familiar with process, contact 99 CS for the procedure.
STEP 2	**REPORT INCIDENT IMMEDIATELY** by secure telephone or in person to your supervisor & USM. USM contacts Wing Information Protection (WIP) 652-7572 / 4434 Note: You may only say, "I'd like to report a possible NDCI" via non-secure means.
STEP 3	**SECURE** affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance, and wait for guidance from USM / WIP. ****Do NOT attempt to forward/respond to/delete any of the info on your own****

Ensure you remove your CAC when leaving your computer unattended.

Backup your data frequently. Ensure you have backups of **mission critical data.**
Option to backup ANY DATA may not be available if an incident occurs.

****99 CS is NOT responsible for backing up your data.****

Report suspicious activity. Personnel should be mindful of situations that indicate when information may be at risk. Stay **alert** for possible **computer viruses/malicious code attacks** and **persons** asking for potentially sensitive information, e.g., user IDs, passwords, websites or e-mail addresses. Heighten your awareness for signs that your e-mail, shared drive, or other correspondence might have been tampered with or opened.

**** Air Force Personnel will never ask for your password****

NELLIS AFB
NETWORK INCIDENT REPORTING CARD
(Continued)

PHISHING E-MAILS

Step 1	**DO NOT REPLY,** and never provide **ANY** information or click on any links!
Step 2	Right click on email, click "Junk", and then click "Block Sender".
Step 3	Delete all junk email from the junk email box.

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH

A PII Breach is defined as actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to a situation where persons other than authorized users and for any other than authorized purpose have access to PII, whether physical or electronic. PII includes, but is not limited to: SSN, DOB, Mother's maiden name, place of birth, address, etc.

Step 1	**STOP!** Take actions to prevent further loss or compromise, e.g., do not forward the email, share the document, etc.
Step 2	**REPORT INCIDENT IMMEDIATELY** by phone, 652-9821 or email the Nellis AFB FOIA/PA Mailbox; nellis.foia@us.af.mil, Unit Privacy Act Monitor and your USM.
Step 3	Base Privacy Act Manager will validate report and submit to USCERTS and senior leadership within 24 hours of breach discovery.

CPCON LEVELS

CPCON 5	**VERY LOW:** Users may experience disruptions in service or access to physical spaces. Priority focus is all functions.
CPCON 4	**LOW:** Users may experience disruptions in service or access to physical spaces. Priority focus is all functions.
CPCON 3	**MEDIUM:** Users may experience disruptions in service or access to physical spaces. Priority focus is critical, essential, and support functions.
CPCON 2	**HIGH:** Users may experience disruptions in service or access to physical spaces. Priority focus is critical and essential functions.
CPCON 1	**VERY HIGH:** Users may experience disruptions in service or access to physical spaces. Priority focus is critical functions.

MY CYBERSECURITY LIAISONS (CL) ARE:

MY COMMANDER'S SUPPORT STAFF (CSS) ARE:

MY UNIT SECURITY MANAGERS (USM) ARE:

Helpful Phone Numbers:

Nellis Comm Focal Point (CFP): 652-2666, Opt 1
Wing Cybersecurity Office (WCO): 652-7039
Wing Information Protection (WIP): 652-7572/4434

DISPLAY / POST THIS CARD NEAR EVERY COMPUTER WORKSTATION

NELLISAFBVA17-1, 20240104 , Prescribed: AFI17-101 OPR: 99 ABW/CCCE RELEASEBILITY: There are no releasability restrictions on this publication.