OIX GATEWAY HONOLULU HI SUCCESSFUL PROCESSING REPORT: OCTOBER 2020 CYBERSECURITY AWARENESS MONTH//
GOES MSG_ID: 510001756336

RTTUZYUW RHOIAAA0001 2681922-UUUU--RHSSSUU.
ZNR UUUUU
R 241914Z SEP 20 MID510001756336U
FM CNO WASHINGTON DC
TO CNO WASHINGTON DC
INFO CNO WASHINGTON DC
BT
UNCLAS

NAVADMIN 265/20

PASS TO OFFICE CODES:
FM CNO WASHINGTON DC//N2N6//
INFO CNO WASHINGTON DC//N2N6//
MSGID/NAVADMIN/CNO WASHINGTON DC/N2N6/SEP//

SUBJ/OCTOBER 2020 CYBERSECURITY AWARENESS MONTH//

POC/PETITT/OPNAV N2N6G/TEL: (571) 256-8465
/EMAIL: DAVID.PETITT.CTR(AT)NAVY.MIL//

RMKS/1. October is National Cybersecurity Awareness Month. While cybersecurity is always a Navy priority, we increase our focus on it during October to remind you of its importance, and to equip you with tools to safeguard the Navy at work and defend yourself at home.

2. To win across the full range of military operations in this era of Great Power Competition, we must connect Navy and Joint sensors and shooters in a battle network that enables our forces to get from threat detection to decisive action as quickly as possible. The systems, networks and data that enable this capability are as critical as weapons without them we cannot compete, deter, and win.

3. Our adversaries understand this. They have become more confident in challenging us below the level of military conflict by stealing our data, and developing ways to compromise Navy systems and networks, including those that control our ships, aircraft, weapons, and infrastructure.

4. The connectedness we need increases our lethality but it also increases shared risk. With a foothold inside our networks, adversaries can quickly move to more vital targets. When they have this capability, a mistake by one individual puts others at risk. Because the stakes are so high in this networked environment, adhering to cybersecurity policies and best practices requires an ALL HANDS approach to keep the Navy and our nation safe. Cybersecurity best practices also provide protection against hackers intent on exploiting smart phones, personal computers and other consumer

computing devices.

5. During October, we will publish content on the Navys social media platform and on the American Forces Network as part of the national campaign for raising cybersecurity awareness. Use these materials to understand the threats we face and how to protect against them. Each week will have a different theme:
    a. Week One: If You Connect It, Protect
    b. Week Two: Securing Devices at Home and Work
    c. Week Three: Secure Teleworking
    d. Week Four: The Future of Connected Devices

6. For easy access to this content, go to https://www.doncio.navy.mil and select Cybersecurity Awareness Month announcement. Many of the excellent cybersecurity resources from the Cybersecurity and Infrastructure Security Agency will be reposted at https://www.cisa.gov/national-cyber-security -awareness-month.

7. We have invested heavily in capabilities to protect Navy networks, systems, and data, and our cybersecurity defenders stop attacks daily, but you are part of the cyber fight too. Every time you log onto a system or network at home or at work you are on the front lines of the cyber battlespace. I appreciate your commitment to keeping the Navy safe by following cybersecurity best practices and policy.

8. Request widest dissemination. This NAVADMIN will remain in effect until cancelled or superseded.

9. Released by VADM Jeffrey E. Trussler, Deputy Chief of Naval Operations for Information Warfare, OPNAV N2N6.//
BT
#0001
NNNN
<DmdsSecurity>UNCLASSIFIED//</DmdsSecurity>
<DmdsReleaser>RIOS.ANA.JUDITH.1293980663</DmdsReleaser>