R 052359Z MAR 25 MID120001767785U
FM COMDT COGARD WASHINGTON DC
TO ALCOAST
BT
UNCLAS
ALCOAST 105/25
SSIC 5510
SUBJ: DIRECT ACCESS DATA BREACH AND OPERATING STATUS - SITREP 1
A. COMDT COGARD WASHINGTON DC 182347Z FEB 25/ALCOAST 074/25
1. Following the security breach announced in REF (A), Direct Access (DA) was fully restored on Wednesday, 19 February. The breach has been mitigated, all payroll actions are on schedule, and DA is being closely monitored with enhanced security capabilities. An investigation of the breach remains ongoing.
2. To further bolster DA's cybersecurity posture, significant efforts are underway to implement multi-factor authentication (MFA). Once implemented, Common Access Card (CAC) holders with a CGOne account will be required to log in via CAC credentials. Non-CAC users will log in with username and password credentials combined with a one-time passcode (OTP) validated through a mobile phone authenticator application, phone call, or text (SMS) message.
   a. Timeline. MFA-enabled services are scheduled for deployment on 17 March 2025 with phased implementation for different MFA methods as required by use case.
   b. What to expect. Implementation of MFA involves highly complex back-end configuration changes that should be unnoticeable to users within the DA application. However, users will experience a new login screen with specific MFA selections for Coast Guard CAC users and non-CAC users. Specific login actions and details for each user group are noted below.
   c. Coast Guard CAC Users. All CAC users with a CGOne account will select the CAC-enabled option on the new DA login screen and follow prompts to authenticate. Employer Identification (EMPLID) number and password access will be disabled for CGOne account holders.
   d. Non-CAC Users. Generally, non-CAC DA users consist of retirees, annuitants, and beneficiaries. Of note, this includes individuals who may have a CAC but work for another government agency and do not have a CGOne Network account. MFA implementation for non-CAC users will consist of two key phases.
   e. Non-CAC Users (No CGOne Account) - Phase I (17 March). The first phase involves back-end changes requiring a new password reset. Non-CAC users will receive instructions with a pre-generated (temporary) password sent to their current email on file within DA (if available). A notice with brief instructions on how to obtain a pre-generated password and perform a password reset will be posted on the new DA login screen for users who do not receive the email. Once reset, non-CAC users will log in via EMPLID and the new password until Phase II is initiated.
   f. Non-CAC Users (No CGOne Account) - Phase II. The second phase incorporates use of an OTP sent to an alternate device. Non-CAC users will receive additional instructions via email or will see applicable guidance on the DA login screen when this feature becomes available.

3. Additional Guidance. All users should ensure their contact information is current in DA. With tax filing season closing soon, users should download tax forms as soon as possible. The necessary system-wide password resets may cause unintended delays in receiving help desk assistance. Ensuring contact information is current supports self-service password reset options and reduces call volumes for all customer support activities.

a. Non-CAC users in receipt of this message are strongly encouraged to log into DA now and ensure all contact information is current, specifically their email address(s). User guides and self-service options for DA are available on the U.S. Coast Guard Pay and Personnel Center (PPC) website at:
(Copy and Paste Below URL into Browser)

https://www.dcms.uscg.mil/ppc/pd/da/

b. It is highly encouraged that anyone in receipt of this message relay it to any retiree, annuitant, or beneficiary (non-CAC user) they may be in contact with to maximize awareness.

c. All Chief Information Officer (CIO) Orders remain in effect per REF (A). For clarification, users with Elevated Roles shall not access DA's public facing website directly from personal device browsers, including from government-issued mobile devices. Accessing DA from any device via the Manta Virtual Desktop application remains authorized.

d. Users are expected to uphold the highest standards of cybersecurity and immediately report suspicious activity to the Cyber Security Operations Center (CSOC), by calling 1-866-424-2478 or via email (CGCYBER-SOC@uscg.mil).

4. Additional Security Measures. As an added layer of security, users can expect to receive a notification via the email address on file in DA whenever bank account information is modified in any capacity, alerting users to take appropriate action if necessary. Further, guidance for enrolling in Identity Protection Services for those directly impacted by this incident is forthcoming. In the interim, users may contact the Office of Privacy Management, COMDT (CG-6P), at any time via email (uscgprivacyincidents@uscg.mil) for additional guidance on protecting personal information.

5. CG-6, the C5I Service Center, CGCYBER, and PPC remain acutely focused on protecting our workforce's sensitive information and supporting military readiness by ensuring HR and payroll systems remain secure and fully operational.

6. POCs: Mrs. Lynnae J. Tyler, COMDT (CG-681) Lynnae.J.Tyler2@uscg.mil or CDR Marlon L. Heron, COMDT (CG-681), Marlon.L.Heron@uscg.mil.

7. RDML Russell E. Dash, Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (CG-6), sends.

8. Internet release is authorized.