United States Coast Guard
U.S. Department of Homeland Security

07 JUN 2023
FM: CHDIRAUX
TO: ALAUX
ALAUX 024/23

Subj: WARNING - MALICIOUS EMAIL / ATTEMPTED PHISHING INVOLVING SF-86 COLLECTION FOR BACKGROUND INVESTIGATIONS

---

1. The Defense Counterintelligence and Security Agency (DCSA) has been made aware of a sophisticated malicious phishing email circulating which references the collection of an "SF-86_F" form or an SF-86 addendum (an example of the email is attached). Please do not engage with this email and advise others not to engage with it. You should delete it immediately if received and report that to your Flotilla Communications Services Staff Officer (FSO-CS) and Flotilla Commander (FC) for collation and relay to your District Director of Auxiliary (DIRAUX). This email is NOT coming from DCSA, or any other vetting or Personnel Security entity in the U.S. Government or Department of Defense. IT professionals have confirmed that the email is malicious in nature.

2. Although the language in the email targets DoD employees, it has been sent to non-DoD associated individuals as well. This ALAUX is meant to ensure awareness among Coast Guard Auxiliarists.

3. The message from DCSA containing the malicious email example is attached to this message for your convenience.

4. Internet release is authorized.

---

***For many reasons including the value of keeping communication lines clear and open as well as facilitating access to training and educational tools, all Auxiliarists are urged to have their own email address and to keep it updated in AUXDATA.***

---

*All ALAUX's are posted on the Chief Director of Auxiliary web site located at: CHDIRAUX ALAUX

---

If you have a question regarding this ALAUX, please seek resolution within your Chain of Leadership and Management (COLM) including up to your servicing District Director of Auxiliary (DIRAUX). If your question still cannot be resolved after that, then please email CGAUX@uscg.mil.

Phishing attempt

DCSA has been made aware of a sophisticated malicious phishing email circulating which references the collection of an “SF-86_F” or an SF-86 (an example of the email is below). Please do not engage with this email and advise your staff not to engage with it; you should report it to your security office or cyber security team and delete it immediately if received. This email is **NOT** coming from DCSA, or any other vetting or Personnel Security entity in the U.S. Government or Department of Defense. IT professionals have confirmed that the email is malicious in nature.

In some cases the link is associated with an individual who **is** listed in the DOD phone directory and in a few cases, that individual has turned out to be an actual security manager. This email has a fairly high ability to potentially trick individuals because they may not know that an SF-86F does not exist, and because the site that it leads to as well as the email look legitimate enough to get people to act, especially with the quick suspense date in the subject line.

The following is an example of the email:

**From:** no-reply@sharepoint-gov.us <no-reply@sharepoint-gov.us>
**Sent:** Saturday, May 27, 2023 3:23 AM
**To:**
**Subject:** ***ACTION: Mandatory SF-86 Addendum for all DoD employees DUE NLT COB 02 JUNE 2023 ***

ALCON,

Due to a number of high profile spillages and intelligence leaks, all federal and DoD Contract employees are required to view the "DoD Reporting and You" powerpoint training and respond to a six question self-report addendum to their SF-86.

If your response is "yes" to any of the addendum questions, you will need to fill out a SF86_F form for each affirmative answer.

The training and addendum questionnaire can be found here: SF-86 Addendum (this is where the malicious link generally is)