Phishing is a type of fraud that uses deceptive e-mails, websites, text messages and/or telephone calls to gather personal, financial and confidential information for fraudulent purposes and/or unauthorized access. Phishing campaigns normally target a wide variety of people. Spear Phishing is tailored to a specific individual and is normally about a subject that is relevant to the recipient. Whale Phishing targets specific, high ranking individuals within an organization. Vishing is the telephone equivalent to Phishing (e.g., telephone call stating your computer has a virus). Smishing is a form of Phishing that occurs via text message. As phishers are getting better at impersonating trusted entities, learning how to spot the difference between legitimate and fraudulent communications is the best way to prevent a cyber attack to the Government Network and its information assets. The following best practices are in alignment with the Federal Government’s Communications Security Establishment (CSE) guidance on Cyber Hygiene.

The following Best Practices should be considered when responding to e-mail messages, websites, text messages and/or telephone calls:

► Ensure your government-issued computer is available to be patched by following the Always On, Always Connected practice.

► Never disclose your government-issued credentials (e.g., username and password). Government Helpdesk staff (e.g., OCIO IT Service Desk, Financial System Control, etc.) will never ask for your government-issued credentials.

► Never use your government-issued email address for personal use.

► Review the content of the received message. Confirm you know who is sending the message and its tone is consistent for the sender. Confirm the content is relevant to your work and not to an area of interest.

► Do not answer suspicious emails/text messages or provide confidential information requested in emails/text/telephone messages, even if the request appears legitimate. Do not respond to messages asking you to verify your identity/information by clicking on a link, or that you have won a prize/contest or to transfer funds immediately because someone you know is in peril.

► If you receive a suspicious e-mail or text message from a recognized organization or client, contact the legitimate organization or client by another means (e.g., by telephone).

► Verify the authenticity of a website; refer to FYI—Safe Web Browsing.

► Visit the OCIO’s website to see examples of phishing e-mails and websites.

► Employees are encouraged to complete the OCIO’s Online Cyber Security Awareness Course.

► Do not forward a suspicious message to others, including the OCIO IT Service Desk, as this expands the number of e-mail accounts potentially affected.

► Contact the OCIO IT Service Desk (1-709-729-HELP), via telephone, if you have questions about phishing or suspect that you have received a fraudulent e-mail or text message.