Summary: Investigation of Phishing Attack on DOI Email Accounts Resulted in Increased Network Security

Report Date: November 7, 2016

OIG initiated this investigation in January 2016, after multiple OIG employees received a "phishing" email from an internal DOI bureau-level employee. The phishing email was sent from the bureau-level employee's account without their knowledge. When the recipients clicked a link within the email, they were presented with a webpage that appeared to be DOI's standard log-in screen, and were prompted for their username and password. At least two recipients clicked on the link and entered their DOI Gmail (Bison Connect Email System) credentials, thereby unknowingly compromising their accounts. Subsequently for two weeks, more than 1,500 DOI employees received the phishing email, resulting in approximately 100 compromised DOI employee Gmail credentials. The successful phishing attack resulted in illegal access to the DOI network through remote logins on a least eight Gmail accounts.

Our investigation found that the source of the attack was most likely physically located outside the United States, therefore, we turned the information over to the Federal Bureau of Investigation for continued investigation through their National Cyber Investigative Joint Task Force.

As a result of this investigation, the DOI Office of the Chief Information Officer accelerated its existing plan to require two-factor authentication for DOI Gmail access, and completed the transition eleven days after the attack began. By implementing two-factor authentication, DOI ended the attack and it substantially increased the security of DOI's Gmail system, Bison Connect.

This is a summary of a report of investigation that was issued to the DOI Chief Information Officer.