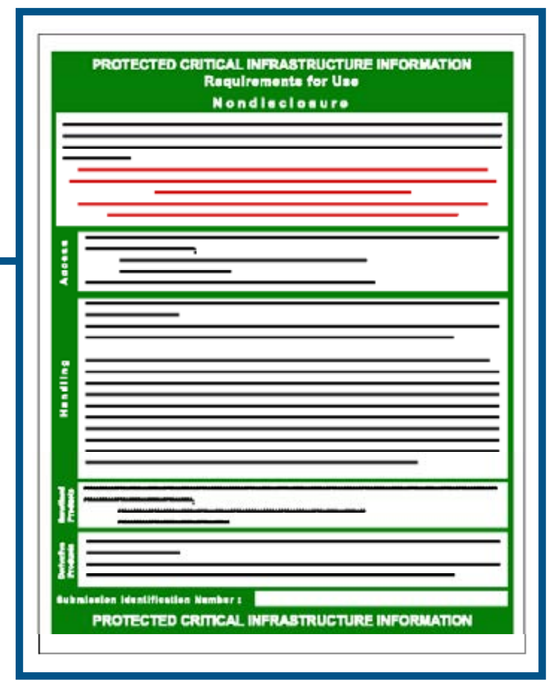
Information Protection Begins With You

PCII
Protected Critical Infrastructure Information

Think Before You Click!
Emailing PCII

1 Check
the **document** to be emailed:

- Has a PCII cover sheet
- Is properly marked with PCII Headers and Footers
- Is password protected using password protection and encryption capabilities in MS Office products or Adobe Acrobat



2 Verify
all **email recipients**

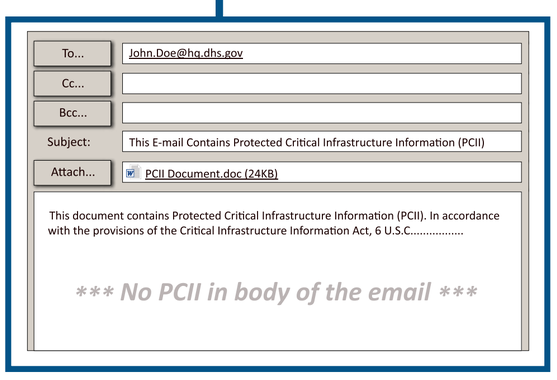
- Using PCIIMS, ensure all recipients are PCII Authorized Users
- Do *not* send PCII to personal, non-employment related email accounts

3 Place
PCII content in the **outgoing email**

- Place in the subject line:

  "***This email contains Protected Critical Infrastructure Information (PCII)"***
- Place in the body of email:

  "This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the 6 U.S.C. § 131 et seq. – The Critical Infrastructure Information Act of 2002 (the CII Act), it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation 6 C.F.R Part 29 and the PCII Program requirements."
- Ensure no PCII is in the body of the email



4 Send
the message and **follow-up**

- If available, send email with PCII over an **encrypted communications** system
- Email the password to the PCII protected document in a separate email
- Contact recipients to verify the PCII was received

Contact the PCII Program Office at PCII-Assist@cisa.dhs.gov for more information