

MEMORANDUM FOR: All Hands

FROM: Joseph F. Klimavicz  
Chief Information Officer  
National Oceanic and Atmospheric Administration

SUBJECT: Protecting Personally Identifiable Information (PII)

Date: February 4, 2010

Security breaches leading to unauthorized disclosure of Personally Identifiable Information (PII) have increased dramatically over the past few years. Over 285 million records *were* compromised nationally in 2009 alone. During the last few months several incidents resulting in unauthorized disclosure of PII have occurred within the Department of Commerce. NOAA must protect the PII entrusted to us.

We have several key technologies in place, such as Laptop full disk encryption, to reduce the risk to NOAA, our employees, contractors, and customers of the potential loss of PII. And we continue to add new technologies, including a near-term enterprise-wide email encryption capability. However, it is important to remember that technology is only one part of the solution. Everyone processing PII must know and follow the policies and procedures for storing, handling, and sharing PII. Specifically:

- Understand NOAA and DOC Policy for handling PII
  - o [http://www.cio.noaa.gov/Policy\\_Programs/ciopol.html](http://www.cio.noaa.gov/Policy_Programs/ciopol.html)
- Encrypt electronic PII whenever possible. All electronic transmission of PII must be encrypted.
- Shred physical PII when it is no longer needed
- Share PII only with authorized users that have a need to know
- Report unauthorized disclosure of PII immediately to the NOAA Computer Incident Response Team (N-CIRT)

<https://www.csp.noaa.gov/noaa/ncirt/itsecreport.xhtml> or (301) 713-9111

Further, DOC initiated a PII processing stand down to review these policies and procedures with all staff that have access to PII. Everyone must protect PII at all times in all forms, physical and electronic. The Secretary has asked that all employees who are responsible for handling and protecting PII be briefed using guidance provided at <http://www.cio.noaa.gov>. Managers must

discuss these points with each member of their organization that is responsible for PII no later than close of business, Friday, February 5, 2010.

Finally, as a citizen and NOAA employee you should be aware that DOC and NOAA have processes in place to respond to loss of PII. The Department has established an Identity Theft Task Force to review every incident involving PII. The task force assesses the risk and develops a response plan designed to ensure everyone affected is adequately protected.

Your attention to this matter is critical to NOAA's success as an organization, and requires that every manager and employee understand and implement all guidance and procedures related to PII.