PII and Email Communications

What is PII?

PII is an acronym that means 'personally identifiable information'. Examples of **PII** would include *but not be limited to* information such as:

- full name,
- Social Security number or employee identification number,
- home address and telephone number,
- vehicle registration number or driver's license number,
- face or fingerprints,
- Credit card number,
- employment date or retirement eligibility date,
- health status or information,
- personal rights and benefits information
- race, ethnic, religion, or sexual orientation
- mother's maiden name
- permit number

Essentially **PII** is any information that can be used to put an individual at risk for identity theft, or could compromise their personal privacy in some way. Most people concentrate on the major bits of information – but do not realize that a composite of individual pieces of information that form a mosaic (more complete picture) can also be damaging in the wrong hands (An example would be: your birth date plus your mother's maiden name)

What about email and PII?

Email systems do not currently qualify as Privacy Act systems. Instead, they have been identified by OMB as 'general support systems' used to transmit information. That doesn't mean there is no risk.

Think risk isn't an issue? Think again. Here are two examples that have actually happened within FWS:

1) Two bureau employees who have similar names receive each others emails because of operator error.
2) An employee receives medical information about another employee even though it was addressed to the correct individual – an apparent 'glitch' in the email system.

Of course, **PII** may be readily transmitted via email and there is a risk that the information may either be captured 'en route' or provided to the wrong party (either by mistake or purposefully). When this happens, or if the person receiving the information does not have the proper approval to collect or maintain the information (see the Privacy Act of 1974), the Government may have what is called a 'breach' situation. Scanning technology in use by the Security office in FWS often catches such inappropriate transmissions.

When an inappropriate transmission is detected, it is reported to the bureau Security Officer, the bureau Privacy Act Officer, and the Department. Credit monitoring may be extended to affected employees - and your office pays for it. In instances where an individual injury or damage has occurred due to negligence or intent - the individual may be liable.

When it comes to sending **PII** over email**,** remember:

"Easy to do – but hard to pay for."