

HSO SPOTLIGHT No. 008-2007: Operations Security (OPSEC)

What is the issue:	Operations Security (OPSEC)
Why do we need this?:	Protection of critical program and personal information from exploitation and unauthorized or inadvertent release
Who is impacted?:	Everyone
What does the HSO need to do?:	Distribute to your organizational personnel

Operations Security is a process that identifies, controls, and protects sensitive, but unclassified, information about a mission, operation, or activity. By recognizing and protecting sensitive information, potential adversaries can be denied the tools that would allow them to compromise or interrupt an organization's mission, operation, or activity.

Employees are reminded of the need to be aware of and protect sensitive work and personal information and to not dispose of it in the recycle or trash receptacles. It should be properly shredded or placed in plain brown burn bags and disposed of appropriately. Some examples of sensitive information are:

DOE travel itineraries	Personally Identifiable Information such as:
VIP/distinguished visitor schedules	- Social Security Numbers
Building plans/facilities engineering	- Place of birth
Patents and scientific papers	- Date of birth
Procurement/contractual information	- Mother's maiden name
DOE budget information	- Biometric record (fingerprint, iris scan, DNA)
Username and passwords	- Medical history information
Financial information (credit card and bank account numbers)	- Criminal history
	- Financial information
	- Security clearance history or related information
	- Employment history

If you have any questions, please contact either Jack Harley at 3-4031 or Brenda Swiger at 3-4440..