

Information Protection Chart

Most Protected

Least Protected

UCNI	PII	OUO	Privacy Act	Company Private	OPSEC
<p>Concerns atomic energy defense programs and pertains to (1) the design of nuclear production or utilization facilities; (2) security measures for the physical protection of these facilities or for nuclear material in these facilities or in transit; (3) the design, manufacture or use of any nuclear weapon or component if the information in question was once classified as Restricted Data and if conditions of an <i>adverse effects test</i> are met. The <i>adverse effects test</i> provides for control of the above categories of information as UCNI if it is determined that unauthorized distribution of the information could reasonably be expected to have a significant adverse effect on the health and safety of the public, or the common defense and security, by significantly increasing the likelihood of the illegal production of a nuclear weapon or the theft, diversion, or sabotage of nuclear material, equipment, or facilities.</p> <ul style="list-style-type: none"> ▪ Obtain a determination from an authorized derivative classifier/UCNI reviewing official. ▪ Must transmit using Entrust. ▪ Marked Unclassified Controlled Nuclear Information; requires cover stamp. ▪ See SP6-024 or DOE orders for marking, protecting, destroying. 	<p>Company-generated documents and reports, both hard copy and electronic, containing information protected under the Privacy Act and elevated to PII status.</p> <ol style="list-style-type: none"> 1. Social security numbers in any form. 2. Place of birth associated with an individual. 3. Date of birth associated with an individual. 4. Mother's maiden name associated with an individual. 5. Biometric record associated with an individual – fingerprint, iris scan, DNA 6. Medical history information associated with an individual – previous diseases, metric information, weight, height, blood pressure 7. Criminal history associated with an individual. 8. Employment history associated with an individual – ratings, disciplinary actions 9. Financial information associated with an individual – credit card numbers, bank account numbers 10. Security clearance history or related information <ul style="list-style-type: none"> ▪ If you are unsure, ask a supervisor. ▪ Must transmit using Entrust. ▪ Marked Personally Identifiable Information. ▪ Destroy by shredding. ▪ See SP3-011. 	<p>OUO information has specific protection requirements defined by DOE. Individuals who work regularly with OUO material should be familiar with these requirements.</p> <p>Determine whether the information could damage governmental, commercial, or private interests if given to someone who does not need it to perform his or her job or other DOE-authorized activity. That decision may already have been made for you if your organization or the Office of Security has issued guidance that states such information is OUO. If no guidance has been issued, then determine whether there is a potential for damage and if the information falls under at least one of the FOIA exemptions 2-9. If so, the document contains OUO information. Most WSI work will fall under Exemption 2, Circumvention of Statute.</p> <ul style="list-style-type: none"> ▪ If unsure, contact a WSI Derivative Classifier. ▪ Must transmit using Entrust or password protection. ▪ Marked Official Use Only; requires cover stamp. ▪ See the DOE and/or WSI OUO pamphlet on the company web site Security Page or DOE orders for marking, protecting, destroying. 	<p>Sensitive personal information is protected under the Privacy Act of 1974. This includes information about an individual's education, financial transactions, medical history, and criminal or employment history if the information contains the employee's name or identifying number, symbol or other identifying indicator assigned to the individual, such as a fingerprint or voiceprint or a photograph <i>unless</i> it has been elevated to be included as <i>Personally Identifiable Information</i>. Includes company-generated documents and reports, both hard copy and electronic, containing this information.</p> <ul style="list-style-type: none"> ▪ If unsure, ask a supervisor. ▪ Transmit using Entrust or password protection when possible. ▪ Marked Privacy Act Information. ▪ Destroy by shredding or send a burn bag for NTS burial. ▪ See SP3-011. 	<p>Company proprietary information that relates to internal company processes such as payroll, budgets, labor relations, wage and salary information, company negotiations, investigations, or other like information not covered under the Privacy Act of 1974.</p> <ul style="list-style-type: none"> ▪ If unsure, ask a supervisor. ▪ Transmit using Entrust or password protection when possible. ▪ Marked Company Private. ▪ Destroy by shredding, send a burn bag for NTS burial, or deposit in an OPSEC bin. ▪ See SP3-011. 	<p>Information, the disclosure of which could reasonably be expected to adversely affect national, DOE, or company security interests. This includes both classified and unclassified information and matter, e.g., Export Controlled Information, Naval Nuclear Propulsion Information, UCNI, OUO, personnel information, and certain unclassified information or matter, as identified in the Elements of Critical Information and Indicators list and the Critical Program Information List.</p> <ul style="list-style-type: none"> ▪ If unsure, ask a supervisor. ▪ Transmit using Entrust or password protection when possible. ▪ Marked OPSEC Material – Destroy by Shredding. ▪ Destroy by shredding, send a burn bag for NTS burial, or deposit in an OPSEC bin. ▪ See SP6-032

For mixed information, always mark and destroy at the highest level.

Note: Intended as a quick reference; refer to the DOE/WSI directives for complete information.