REVISED INFORMATION IMPACT LEVELS

Definition: Impact Levels are defined by potential impact of an event resulting in the loss of confidentiality, integrity or availability of data, systems, or networks.

The security control baseline for all Impact Levels is predicated on moderate confidentiality and moderate integrity as defined by CNSSI 1253 and the FedRAMP Moderate Baseline. Categorize systems IAW DoDI 8510.01 and CNSSI 1253. Availability is determined by mission owner and should be specified in the contract. FedRAMP authorization is the minimum security baseline.

Level #	Maximum Data Type	Information Characterization
2	Non-Controlled Unclassified Information	Unclassified information approved for public release
		Unclassified, not designated as controlled unclassified information (CUI) or critical mission data, but requires some minimal level of access control
4	Controlled Unclassified Information	Requires protection from unauthorized disclosure as established by Executive Order 13556 (Nov 2010); Education, Training, Recruiting, Credit card information for individuals (i.e., PX or MWR events)
		PII, PHI, SSN, Credit card information for individuals, Export Control, FOUO, Law Enforcement Sensitive, Email
5	Controlled Unclassified Information + NSS	National Security Systems and other information requiring a higher level of protection as deemed necessary by the information owner, public law, or other government regulations; dedicated instance required
6	Classified up to SECRET	Pursuant to EO 12958 as amended by EO 13292; classified national security information or pursuant to the Atomic Energy Act of 1954, as amended to be Restricted Data (RD)