Appendix 9 Principles for Classifying Protection Requirement Levels for Information and Communication Systems

Required Protection Levels / Dimension	High	Medium	Basic
Confidentiality	A cyber security incident affecting an information and communication system may result in unauthorized disclosure of information, causing a severe or catastrophic adverse effect on the agency's operations, assets, or reputation.	A cyber security incident affecting an information and communication system may result in unauthorized disclosure of information, causing a serious adverse effect on the agency's operations, assets, or reputation.	A cyber security incident affecting an information and communication system may result in unauthorized disclosure of information, causing a limited adverse effect on the agency's operations, assets, or reputation.
Integrity	A cyber security incident affecting an information and communication system may result in errors in information or unauthorized alteration thereof, causing a severe or catastrophic adverse effect on the agency's operations, assets, or reputation.	A cyber security incident affecting an information and communication system may result in errors in information or unauthorized alteration thereof, causing a serious adverse effect on the agency's operations, assets, or reputation.	A cyber security incident affecting an information and communication system may result in errors in information or unauthorized alteration thereof, causing a limited adverse effect on the agency's operations, assets, or reputation.
Availability	A cyber security incident affecting an information and communication system may result in the interruption of access to, or use of, information or the information and communication system, causing a severe or catastrophic adverse effect on the agency's operations, assets, or reputation.	A cyber security incident affecting an information and communication system may result in the interruption of access to, or use of, information or the information and communication system, causing a serious adverse effect on the agency's operations, assets, or reputation.	A cyber security incident affecting an information and communication system may result in the interruption of access to, or use of, information or the information and communication system, causing a limited adverse effect on the agency's operations, assets, or reputation.
Legal and Regulatory Compliance	Failure to comply with cyber security-related laws and regulations applicable to the establishment or operation of an information and communication system may affect the system and thereby cause a cyber security incident, or adversely affect the lawful rights and interests of	Failure to comply with cyber security-related laws and regulations applicable to the establishment or operation of an information and communication system may affect the system and thereby cause a cyber security incident, or adversely affect the lawful rights and interests of	Other circumstances in which the establishment or operation of an information and communication system is subject to relevant legal requirements.

	others or the fairness and legitimacy of the agency's performance of its duties, and cause the agency's personnel to incur criminal liability.	others or the fairness and legitimacy of the agency's performance of its duties, and subject the agency or its personnel to administrative penalties, disciplinary sanctions, or disciplinary actions.	

Note: The protection requirement level of an information and communication system shall be determined by the highest level among the dimensions of confidentiality, integrity, availability, and legal and regulatory compliance relevant to that system.