

CYBER-TERRAIN SCORING RUBRIC

Federal information and information systems are subject to constant threats that may have varying degrees of impact on organizational operations (including mission, function, image, and reputation), assets, individuals, other organizations, and the Nation. Additionally, these varying impacts can have the effect of compromising the confidentiality, integrity, or availability of information being processed, stored, transported, interfaced with, managed, disseminated, or protected by those systems. Given the significant and growing danger of cyber threats, it is imperative that leaders at all levels of the organization understand their responsibilities for achieving adequate information security and for managing information systems-related to security risks.

To assess the risks associated with operating in a contested environment and interconnected world, it is imperative that organizations understand the mission impact of a complete loss of, or degradation in capability, of a given information technology system. To this end, the following scoring rubric breaks down assessment factors in order to assign a cyber-terrain score, based on an understanding of factors and importance of the system in completing the organization’s mission. It is important to note that a cyber-terrain score may be adjusted over time (temporarily or permanently) based on the emergence of new missions, threats, or the elevated importance of a current mission (whether based on updated intelligence, geographic importance, scope, or applicability).

The following chart gives the person scoring any given system, guidelines as to where certain impact factors should be scored. The chart is not intended to be all inclusive and should only be considered as a recommendation to the individual assigning a cyber-terrain score. Judgement and experience are also two essential factors that an individual should use to guide the assignment of appropriate cyber-terrain scores.

	Description of Impact	Score
1	Possible Loss of Life	10
2	Inability to execute or complete mission	9
3	Degradation of C2	9-7
4	Mission Performance Degradation (Limited, Moderate, Severe)	9, 7, 5
5	Compromise of Personal Health or Privacy Data (PII / PHI)	8
6	Inability to complete full mission	8
7	OPSEC Violation	8
8	Loss of Logistical support	8-6
9	International impact	8-6
10	Economic Impact (Organizational, DoD, National)	8, 6, 4
11	Complete Loss of a System / Application / Infrastructure for greater than 14 days	7
12	Federal Regulation or Law Non-Compliance (other than Privacy & HIPPA/HITECH)	7
13	Adversaries’ capabilities increased	6
14	Loss or effect on associated systems	6
15	Effect on Future Capabilities	5
16	Contractual Non-Compliance	4
17	Public Affairs (Public Incident)	3
18	Compromise of UNCLASS local laptop or stand-alone system	1-2

Value	IMPACT Score Description	Data Compromise	Mission Impact	Information Systems Impact	Effect on Future Capabilities	External to Organization Affect
10	The event or loss of confidentiality, integrity, or availability would be expected to have <u>catastrophic adverse effects on the mission leading to loss of life and complete mission failure.</u>	Of a classification and operational nature as to catastrophically affect the mission. Data protections under the Privacy, HIPPA , and HITECH Acts (PII and PHI)	Possible loss of life	Compromise of an operationally critical system	Immediate and lasting effect s	International effect and impact can be expected
9	The event or loss of confidentiality, integrity, or availability would be expected to have <u>catastrophic adverse effects</u> on the mission leading to complete mission failure.		Inability to perform or complete the mission [whether based on type of system(s) affected, number of users, or targeted user(s)]	Adversely affects other / multiple vital systems		
8	The event or loss of confidentiality, integrity, or availability could be expected to have <u>multiple severe or catastrophic adverse effects</u> on the mission. A severe or catastrophic adverse effect may mean, the threat could cause several severe degradations in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; resulting in major damage to organizational assets; result in major financial loss; or catastrophic harm to individuals involving possible loss of life or serious life threatening injuries.					
7	The event or loss of confidentiality, integrity, or availability could be expected to have <u>a severe or catastrophic adverse effect</u> on the mission. A severe or catastrophic adverse effect may mean the threat could cause a severe degradations in or loss of mission capability to an extent and duration that the organization is not able to perform one of its primary functions.	Data protected by Federal Statutes and Department of Defense Regulation	Inability to execute primary objective of the mission [whether based on type of system(s) affected, number of users, targeted user(s)]	Compromise of a system that advisedly affects or potentially affects another system (e.g.: IDS, IPS, Firewalls)	Potential for lasting effect is very high	National-level impact can be expected (e.g.: media, DHS, etc.)
6	The event or loss of confidentiality, integrity, or availability could be expected to have <u>multiple serious adverse effects</u> on the mission. A serious adverse effect means that the threat event may cause significant degradation in mission capability to an extent and duration that the organization is not able to effectively perform one or more of its primary functions; the effectiveness of the functions are significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or significant harm to individuals that does not involve loss of life or serious life threatening injuries.		Inability to execute primary objective of the mission [whether based on type of system(s) affected, number of users, targeted user(s)]	Compromise of a system that advisedly affects another system. (Any cursory system affected is of a non-critical nature.)	Potential for lasting effect is very high	National-level impact can be expected (e.g.: media, Department of Homeland Security, etc.)
5	The event or loss of confidentiality, integrity, or availability could be expected to have <u>multiple serious adverse effects</u> on the mission. A serious adverse effect means that the threat event may cause significant degradation in mission capability to an extent and duration that the organization is not able to effectively perform one or more of its primary functions; the effectiveness of the functions are significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or significant harm to individuals that does not involve loss of life or serious life threatening injuries. The event or loss of confidentiality, integrity, or availability could be expected to have <u>a serious adverse effect</u> on the mission. A serious adverse effect means that the threat event may cause significant degradation in mission capability to an extent and duration that the organization is not able to effectively perform one of its primary functions; the effectiveness of the function is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or significant harm to individuals that does not involve loss of life or serious life threatening injuries.					

Value	IMPACT Score Description	Data Compromise	Mission Impact	Information Systems Impact	Effect on Future Capabilities	External to Organization Affect
4	The event or loss of confidentiality, integrity, or availability could be expected to have <u>multiple limited adverse effects</u> on the mission. The limited effect may be in the form of mission capability degradation, but the organization is able to perform its primary functions with minor degradation in effectiveness.	Data protected by local regulations	Primary mission objective can still be performed with over-all varying degrees of minor degradation (Regardless of number of systems or users)		Minimal to no future effect will be felt	Internal-only departmental effects can be expected
3	The event or loss of confidentiality, integrity, or availability could be expected to have a <u>limited adverse effect</u> on the mission. The limited effect may be in the form of mission capability degradation, but the organization is able to perform its primary functions with minor degradation in effectiveness.			Any cursory or secondary system affected is of a non-critical nature		
2	The event or loss of confidentiality, integrity, or availability, could be expected to have <u>minor and negligible adverse effects</u> on the mission, organizational operations, organizational assets, individuals, or other organizations.				No effect on future capabilities may be anticipated	No noticeable effect outside immediate team should be expected
1	The event or loss of confidentiality, integrity, or availability, could be expected to have <u>none or negligible adverse effects</u> on the mission, organizational operations, organizational assets, individuals, or other organizations.			Stand-alone system		