Department of the Army
Pamphlet 190–51

Military Police

Risk Analysis for Unclassified Army Resources

Headquarters
Department of the Army
Washington, DC
27 June 2019

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 190–51
Risk Analysis for Unclassified Army Resources

This major revision, dated 27 June 2019—

- Changes the publication title from “Risk Analysis for Army Property” to “Risk Analysis for Unclassified Army Resources” (cover).
- Updates DA Form 7278 (Risk Level Worksheet) (para 1–7*b*).
- Adds risk analysis for arms ammunition and explosives (tables 1–1 and 2–1).
- Adds arms ammunition and explosives relative value of arms ammunition and explosives resources (table 2–10).
- Adjust sum of likelihood rating factors (table 3–18).
- Provides analysis factors for new resource categories in AR 190–51, including U.S. Army Corps of Engineers Civil Works project resources (throughout).

Headquarters
Department of the Army
Washington, DC
27 June 2019

*Department of the Army Pamphlet 190–51

Military Police

Risk Analysis for Unclassified Army Resources

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a major revision.

Summary. This pamphlet presents a risk analysis method designed to assist commanders in meeting local needs and enhancing security using available resources, by use of the U.S. Army Security Management System (Countermeasures) software or DA Form 7278. The results of the risk analysis can be used to determine the minimum level of protection needed to safeguard resources adequately and economically. The level of security adopted will be based upon physical security measures and procedures contained in AR 190–11 or AR 190–51.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to U.S. Army contractors using or handling sensitive or nonsensitive unclassified U.S. Army resources. This publication applies during partial and full mobilization, and during contingency operations.

Proponent and exception authority. The proponent of this pamphlet is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Headquarters, Department of the Army, Office of the Provost Marshal General (DAPM–MPO–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This pamphlet supersedes DA Pam 190–51, dated 30 September 1993.

UNCLASSIFIED

Contents—Continued

Table List

Contents—Continued

Figure List

Glossary

Chapter 1
Risk Analysis

Section I

Introduction

1–1. Purpose
This pamphlet provides guidance for conducting risk analysis for the Army resources listed within. The risk analysis procedure supports the local commander in meeting the responsibility of protecting resources against criminal and terrorist threats in a cost effective manner. It is designed to help security specialists carry out their responsibilities in support of the local commander. It also provides a basis for developing the information required by engineers to provide comprehensive protection for resources based on security engineering principles.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. How to use this pamphlet
a. Establish risk levels for each resource requiring protection. Refer to the instructions in section II of this chapter and the risk factor evaluation tables in chapters 2 and 3 to evaluate risk levels.

b. Refer to AR 190–51 for other resources to determine the appropriate minimum levels of security to implement for the resource to be protected based on the risk level for that resource.

Section II

Risk Analysis

1–5. Purpose of risk analysis
Not all Army resources at all locations require the same degree of protection. Protection of resources must be based on a realistic assessment of the risks associated with the criminal and terrorist threats likely to be directed at the resources in their actual locations. Performing risk analysis for resources allows commanders to establish resource protection appropriate for their value and the likelihood of an attempt to compromise them. The risk analysis allows the commander to prioritize resources so that physical security resources can be applied in the most efficient and cost effective manner possible. The commander should ensure insider threat is included in the threat analysis. Risk analysis also provides the supporting facilities engineering organization with the information required to develop design criteria for construction or equipment installation to provide comprehensive security for a resource.

1–6. Risk
Risk indicates both the impact of the compromise of a resource and the potential for it being compromised. Risk is associated with individual resources and with different types of aggressors.

a. Resources. Risk concerns resources rather than facilities. Facilities are not normally the targets of aggressors, and they should not be the focus of security. Facilities contain security elements for the benefit of resources housed within the facility. Security should be based upon protecting the resources in the facilities. The risk analysis procedure in this pamphlet applies to all of the resource types listed in AR 190–51 and AR 190–11 where it is noted that risk analysis is required. It can also be applied to resource types that are not listed, but which may warrant protection.

b. Components of risk. Risk is composed of the two factors of resource value and likelihood of aggressor activity.

(1) *Resource value.* This risk factor indicates the value or importance of the resource to its user and to the Army. The risk level increases with increasing resource value in this risk analysis model. Chapter 3 addresses resource value in more detail.

(2) *Likelihood.* This factor indicates the attractiveness of the resource to the aggressor and the likelihood that an aggressor will attempt to compromise the resource based on its attractiveness. Risk increases with increasing likelihood of aggression. Chapter3 addresses likelihood in more detail.

c. Aggressors. The risk analysis procedure in this pamphlet considers criminals, protesters, and terrorists, as potential aggressors against Army resources. A risk analysis must consider each potential aggressor category likely to be interested in a resource separately. The different aggressor categories and the different groups of aggressors within each category are necessary for developing the threat definition used by security specialists and engineers to compensate for or design for comprehensive security for resources. In the threat analysis developed from elements of this risk analysis, different tactics, weapons, tools, and explosives are assigned to each aggressor type. Risk levels are established only for the broad categories of criminals and terrorists in this risk analysis. For this analysis, protesters are divided into vandals/activists and extremist protesters which are incorporated into the categories of criminals and terrorists defined below:

(1) *Criminals.* Criminals are divided into unsophisticated criminals, sophisticated criminals, and organized criminal groups for this analysis. Vandals/activists are included under the category of criminals.

(2) *Terrorists.* For this analysis, terrorists are divided into those based in the continental United States, based outside the continental United States, and state sponsored terrorists also based outside the continental United States. Extremist protesters and active shooters are also included under the category of terrorists.

(3) *Spies and Saboteurs.* Planning against these types of aggressors is not included because planning for the other aggressor types is sufficient.

(4) *Insider threat.* The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, active shooter, unauthorized disclosure of national security information, or through loss or degradation of departmental resources or capabilities.

1–7. Risk analysis procedure

The following procedure will be applied to all Army resources being considered for protection, including those in existing facilities and those in facilities yet to be constructed or under major renovation.

a. The risk analysis for resources to be located in new or renovated facilities will be performed during the planning stages of the projects. Including required security features during initial facility planning will result in long–term cost savings and improved security system integration.

b. Consult with operations and intelligence personnel; operation security personnel; the provost marshal or director of emergency services; the facility engineer; local, State, and Federal law enforcement, as necessary; and the users of the resources being analyzed as necessary in performing this analysis.

(1) *Step 1.* Identify the unit or organization owning the resource and the area in which the resource is located. Enter this information in the spaces provided on DA Form 7278 (Risk Level Worksheet).

(2) *Step 2.* Identify the resource for which the analysis is being performed. Enter the category of the resource from table 1–1 and enter a brief description to further identify it. If the identified resource does not fall within one of the categories listed in table 1–1 or if it falls within more than one category, select the category which most closely describes the resource and note the difference in the resource description. Enter each resource category and its description in the space provided on DA Form 7278. Analyze each resource separately.

(3) *Step 3.* Determine resource value. Evaluate the appropriate resource value rating factors and determine the resource value rating for each resource as described in chapter 2.

(4) *Step 4.* Determine likelihood of aggression. For each applicable aggressor type and for each resource, evaluate the appropriate likelihood rating factors as described in chapter 3. Determine the highest likelihood ratings for criminals and terrorists as described in chapter 3.

(5) *Step 5.* Determine the risk levels for resources. Use table 1–2 to determine risk levels for each resource based on its value rating and the likelihood ratings for criminals and terrorists as determined in chapters3. Read the matrix (table 2–2) across from the applicable value rating and down from the applicable likelihood rating. The risk level is at the intersection of the two ratings. Enter the risk levels for criminals and terrorists in the spaces provided on DA Form 7278. Figure 1–1 is an example of a completed analysis.

(6) *Step 6.* With the risk level for each resource, refer to AR 190–51 to determine the minimum physical protective measures and security procedural measures.

Table 1–1
Resource categories

Category	Description
A	Aircraft and components including unmanned aircraft systems.
B	Vehicles and carriage–mounted or towed weapon systems.

Table 1–1
Resource categories—Continued

Category	Description
C	Communications and electronics equipment, forward repair systems, standard automotive tool sets, night vision devices and other high value optical devices, high-value precision equipment, and launched electrode stun devices.
D	Organizational clothing and individual equipment.
E	Subsistence items.
F	Repair parts.
G	Petroleum, oils, and lubricants.
H	Facility engineering supply, construction material storage areas, and industrial and utility equipment.
I	Audiovisual equipment, training devices, and sub-caliber devices.
J	Controlled cryptographic items.
K	On-post public and privatized utilities.
L	Air items and airdrop systems, and personnel and cargo parachute systems including associated ancillary items.
M	U.S. Army Corps of Engineers (USACE) Civil Works (CW) project resources.
N	Arms, ammunition, and explosives (AA&E).
O	Medical and medical research resources.

Table 1–2
Risk level matrix

Resource value rating	Aggressor likelihood rating				
	Very low	Low	Medium	High	Very high
Very low (VL)	I	I	I	II	II
Low (L)	I	I	II	II	II
Medium (M)	I	II	II	II	III
High (H)	II	II	II	III	III
Very high (VH)	II	II	III	III	III

RISK LEVEL WORKSHEET

Unit or Organization: **(Insert Unit Information)**	Inspected Resource: **Tactical Vehicles**	Analyst: **(First, Last Name)**
Resource Location: **(dd/mm/year)**	Resource Category: **B**	Date: **(dd/mm/year)**

Resource Value Factors								Aggressor Likelihood Factors												
Criticality to Army's Mission (Table 2-2)	Criticality to User's Mission (Table 2-3)	ResourceReplaceability (Tables 2-4 or 2-19 for USACE	Relative Value (Tables 2-5 to 2-18)	Sum of Value Ratings (Table 2-20)	Resource Value Rating (Table 2-20)			Resource Profile (Table 3-3)	Usefulness for Resource with Cash Value (Table 3-4)	Usefulness to Aggressor Goals (Table 3-5)	Publicity Value (Table 3-6)	Resource Availability (Table 3-7)	Local Incidents in the Past (Table 3-8)	Nearby Incidents in the Past (Table 3-9)	Potential for Future Incidents (Table 3-10)	Accessibility (Tables 3-11 to 3-14)	Effectiveness of Law Enforcement (Table 3-15)	Deterrence (Tables 3-16 or 3-17)	Sum of Likelihood Factors (Table 3-18)
Resource Ratings																				
0	3	2	3	8	L	X	Unsophisticated Criminals	5	3	2	2	3	2	1	2	5	4	5	34
Description:						X	Sophisticated Criminals	5	5	2	2	3	2	1	2	5	4	5	36
2 LMTVs 2 HMMWVs 2 APCs						X	Organized Criminal Groups	5	5	2	2	3	2	1	2	5	4	5	36
						X	Domestic Terrorists	5	5	2	3	3	2	1	2	5	4	5	37
						X	International Terrorists	5	5	2	3	3	2	1	2	5	4	5	37
						X	State Sponsored Terrorists	5	5	2	3	3	2	1	2	5	4	5	37
						X	Insider Threat	5	5	3	3	3	2	1	3	5	5	5	40
																		Highest Aggressor Group Likelihood Factors		**40**
																		Aggressor Likelihood Rating (Table 3-18)		**H**
																		Risk Level (Value and Likelihood Combined) (Table 1-2)		**II**

Figure 1–1. Resource value determination

Chapter 2
Recourse Value Determination

2–1. Measurement of resource value

Resource value is evaluated based on value rating factors which include mission criticality to both the Army and the resource's user, the replaceability of the resource, and a measure of the resource's relative value to its user. Evaluate each value rating factor as described below using the applicable value rating tables.

2–2. Evaluation procedure

a. Select applicable value rating tables. Refer to table 2–1 to determine which value rating tables apply for each resource category.

b. Evaluate value rating factors. Select the entry from each value rating table which most closely applies to the resource. Record the numerical values for the value rating factors in the spaces provided on DA Form 7278.

c. Establish value rating. Refer to guidance in paragraph 2–4.

Table 2–1
Resource value rating factor table applicability

Resource category	Applicable table numbers			
A. Aircraft and components including unmanned aerial systems	2–2	2–3	2–4	2–5
B. Vehicles and carriage–mounted or towed weapon systems	2–2	2–3	2–4	2–6
C. Communications and electronics equipment, forward repair systems, standard automotive tool sets, night vision devices and other high value optical devices, high-value precision equipment, and launched electrode stun devices	2–2	2–3	2–4	2–8
D. Organizational clothing and individual equipment	2–2	2–3	2–4	2–8
E. Subsistence items	2–2	2–3	2–4	2–8
F. Repair parts	2–2	2–3	2–4	2–8
G. Petroleum, oils, and lubricants	2–2	2–3	2–4	2–7
H. Facility engineering supply, construction material storage areas, and industrial and utility equipment	2–2	2–3	2–4	2–8
I. Audiovisual equipment, training devices, and sub-caliber devices	2–2	2–3	2–4	2–8
J. Controlled cryptographic items	2–2	2–3	2–4	2–9
K. On-post public and privatized utilities	2–2	2–3	2–4	2–8
L. Air items and airdrop systems, and personnel and cargo parachute systems including associated ancillary items	2–2	2–3	2–4	2–8
M. USACE CW project resources (select only one table for relative value)	2–2	2–3	2–19	2–11 through 2–18
N. AA&E	2–2	2–3	2–4	2–10
O. Medical and medical research resources	2–2	2–3	2–4	2–8

2–3. Value rating factors

a. Criticality to Army's mission. This factor addresses the criticality of the resource in its support of the Army's capability to mobilize and fight a war. Considering this factor ensures that resources which are critical to Army readiness receive highest priority. Evaluate this factor using table 2–2.

Table 2–2
Criticality to Army's mission

Loss impact	Value rating factor
The loss, theft, destruction, or misuse of the resource could have insignificant impact on the Army's mission.	0
The loss, theft, destruction, or misuse of the asset resource could have significant impact on the Army's mission on a regional level.	1
The loss, theft, destruction, or misuse of the resource could compromise the infrastructure of the Army's mission.	2
The loss, theft, destruction, or misuse of the resource could impact the tactical capability of the Army's mission.	3
The loss, theft, destruction, or misuse of the resource could be expected to harm the operational capability of the Army's mission.	4
The loss, theft, destruction, or misuse of the resource could result in great harm to the strategic capability of the Army's mission.	5

b. Criticality to user's mission.

(1) This factor addresses the criticality of the resource in its support of its user's mission. It accounts for the fact that some resources may be critical to their user's mission, but not to the overall Army mission. An example of such a resource could be kitchen equipment in the officers' club. The equipment may be critical to the club's mission, but is unlikely to be critical to the war-fighting mission.

(2) In the case of applying this table to USACE CW project resources, this factor will address the criticality of the CW project resource in its support of the USACE mission. USACE mission being defined herein as the CW project's "authorized purpose". Considering this factor ensures that CW project resources which are critical to USACE receive high priority within USACE's risk based decision making processes. Assume a national level perspective, verses a local level perspective, when determining the value of this factor. Evaluate this factor using table 2–3.

Table 2–3
Criticality to user's mission

Loss impact	Value rating factor
The loss, theft, destruction, or misuse of the resource would have no significant effect on operations, output, production, or service.	0
The loss, theft, destruction, or misuse of the resource would result in halting operations within 1 month or would result in a 10 percent curtailment of output, production, or service.	1
The loss, theft, destruction, or misuse of the resource would result in halting operations within 2 weeks or would result in a 25 percent curtailment of output, production, or service.	2
The loss, theft, destruction, or misuse of the resource would result in halting operations within 1 week or would result in a 50 percent curtailment of output, production, or service.	3
The loss, theft, destruction, or misuse of the resource would result in halting operations within 1 day or would result in a 75 percent curtailment of output, production, or service.	4
The loss, theft, destruction, or misuse of the resource would result in immediately halting operations, output, production, or service.	5

c. Resource replaceability. This factor addresses the time required to replace resources which have been compromised. Replacement can be either in-kind or with a reasonable substitute and can be either temporary or permanent. This factor accounts for the impact of delay in replacement of resources on the user's mission. Evaluate this factor using table 2–4.

Table 2–4
Resource replaceability

Replacement time	Value rating factor
Can be replaced within 24 hours.	0
Can be replaced within 24 to 72 hours.	1
Can be replaced within 72 hours to 1 week.	2
Can be replaced within 1 week to 1 month.	3
Can be replaced within 1 to 6 months.	4
Can be replaced within more than 6 months.	5

d. Relative resource value. This factor provides a measure of the relative value of a resource based on the cost of the resource or other measures of value appropriate for particular resource categories. Different tables are used to evaluate the relative values of different resource categories in the most appropriate ways of measuring value for the various resource categories. The applicable tables are indicated in table 3–1. Write the number of the table chosen in the space provided on DA Form 7278.

(1) *Relative value of aircraft.* The relative value is measured based on the number of aircraft and the presence of attack aircraft. Evaluate relative value of these resources using table 2–5.

Table 2–5
Relative value of aircraft

Resource amounts	Value rating factor
Less than 5 aircraft with no attack aircraft.	0
Less than 5 aircraft and include attack aircraft.	1
5 to 10 aircraft with no attack aircraft.	2
5 to 10 aircraft and include attack aircraft.	3
Ten or more aircraft with no attack aircraft.	4
Ten or more aircraft and includes attack aircraft.	5

(2) *Relative value of vehicles.* The relative value is based on the number of vehicles and the presence of tactical vehicles and vehicles with carriage–mounted or towed weapons systems. Evaluate relative value of these resources using table 2–6.

Table 2–6
Relative value of vehicles

Resource amounts	Value rating factor
Less than 20 vehicles. No tactical vehicles or carriage–mounted or towed weapons systems.	0
Less than 20 vehicles. Includes tactical vehicles. Does not include carriage– mounted or towed weapons systems.	1
Less than 20 vehicles. Includes carriage–mounted or towed weapons systems.	2
Twenty or more vehicles. No tactical vehicles or carriage–mounted or towed weapons systems.	3
Twenty or more vehicles. Includes tactical vehicles. Does not include carriage–mounted or towed weapons systems.	4
Twenty or more vehicles. Includes carriage–mounted or towed weapons systems.	5

(3) *Relative value of petroleum, oils, and lubricants.* The relative value is based on the quantity being stored. Evaluate relative value of these resources using table 2–7.

Table 2–7
Relative value of petroleum, oils, and lubricants

Resource quantity	Value rating factor
Less than 50,000 gallons.	1
Between 50,000 and 150,000 gallons.	2
Between 150,001 and 500,000 gallons.	3
Between 500,001 and 1,000,000 million gallons.	4
More than 1,000,000 gallons.	5

(4) *Relative value of other resources.* Relative value of resources not included in the tables above is evaluated based upon monetary value. The monetary value may be determined for an inventory of resources or for individual resources, whichever is most appropriate for the quantity of the resources present in the inspectable area being analyzed. Actual quantity of the resources is accounted for in considering the mission criticality of the resources to the Army and the user. Evaluate relative value of these resources using table 2–8.

Table 2–8
Relative value of other resources

Total inventory cost	Value rating factor
Less than $100,000, or the value of an individual resource is less than $10,000.	1

Table 2–8
Relative value of other resources—Continued

Total inventory cost	Value rating factor
Between $100,000 and $250,000, or the value of an individual resource is between $10,000 and $25,000.	2
Between $250,000 and $500,000, or the value of an individual resource is between $25,000 and $50,000.	3
Between $500,000 and $1,000,000, or the value of an individual resource is between $50,000 and $100,000.	4
More than $1,000,000, or the value of an individual resource is more than $100,000.	5

(5) *Relative value of controlled cryptographic items.* The relative value of controlled cryptographic items is determined based on the degree of sensitivity of the information processed with the equipment. Evaluate relative value of these assets using table 2–9.

Table 2–9
Relative value of controlled cryptographic items

Information sensitivity	Value rating factor
For Official Use Only	1
Confidential	2
Secret	3
Top Secret	4
Sensitive Compartmented Information	5

(6) *Relative value of arms, ammunition, and explosives resources.* The value is based on the loss of category I through IV AA&E assets described in AR 190–11. Evaluate the relative value using table 2–10.

Table 2–10
Relative Value of arms ammunition and explosives

Resource amounts	Value rating factor
Category IV less than 50 weapons or 50 kg net explosive weight	1
Category IV more than 50 weapons or 50 kg net explosive weight	2
Category III weapons or explosive	3
Category II weapons or explosive	4
Category I weapons or explosive	5

(7) *Relative value of U.S. Army Corps of Engineers Civil Works project resources.* The USACE CW project resources requiring a risk assessment encompass the spillway gate structure, outlet works structure, intake structure, Service Bridge, embankment, powerhouse, powerhouse control room, unescorted public accessible powerhouse visitor center, switchyard, navigation lock, levee drainage structure, and levee pumping station. To determine the value rating factor of a USACE CW project resource, obtain the project specific Critical Infrastructure Protection and Resilience Program Consequence Topic Screen data and use tables 2–11 through 2–18. In most cases, multiple tables will apply to a CW project resource. Use the table that has the greater rating value factor. Enter the number in DA Form 7278.

Table 2–11
U.S. Army Corps of Engineers—relative value of total economic impact

Total economic impact	Value rating factor
Less than $500 million	1
Greater than or equal to $500 million but less than $1 billion	2
Greater than or equal to $1 billion but less than or equal to $10 billion	3
Greater than or equal to $10 billion but less than $20 billion	4
Greater than or equal to $20 billion	5

Table 2–12
U.S. Army Corps of Engineers—relative value of water supply

Population served	Value rating factor
Less than 1,000	1
Greater than or equal to 1,000 but less than 15,000	2
Greater than or equal to 15,000 but less than or equal to 50,000	3
Greater than or equal to 50,000 but less than or equal to 125,000	4
Greater than 125,000	5

Table 2–13
U.S. Army Corps of Engineers—relative value of irrigation water

Annual water delivery	Value rating factor
Less than 999 acre-feet	1
Greater than or equal to 1,000 acre-feet but less than 10,000 acre-feet	2
Greater than or equal to 10,000 acre-feet but less than 100,000 acre-feet	3
Greater than or equal to 100,000 acre-feet but less than 1 million acre-feet	4
Greater than 1 million acre-feet	5

Table 2–14
U.S. Army Corps of Engineers—relative value of hydropower generation

Generating capacity	Value rating factor
Less than 25 megawatts (MW)	1
Greater than or equal to 25 MW but less than 50 MW	2
Greater than or equal to 50 MW but less than 300 MW	3
Greater than or equal to 300 MW but less than 1,000 MW	4
Greater than 1,000 MW	5

Table 2–15
U.S. Army Corps of Engineers—relative value of flood damage reduction

Annual flood damage reduction	Value rating factor
Less than $10 million	1
Greater than or equal to $10 million but less than $50 million	2
Greater than or equal to $50 million but less than $100 million	3

Table 2–15
U.S. Army Corps of Engineers—relative value of flood damage reduction—Continued

Annual flood damage reduction	Value rating factor
Greater than or equal to $100 million but less than $200 million	4
Greater than or equal to $200 million	5

Table 2–16
U.S. Army Corps of Engineers—relative value of navigation

Navigation tonnage	Value rating factor
Less than 500 kilotons (kt)	1
Greater than or equal to 500 kt but less than or equal to 3,125 kt	2
Greater than or equal to 3,125 kt but less than or equal to 12,500 kt	3
Greater than or equal to 12,500 kt but less than or equal to 4 million kt	4
Greater than or equal to 4 million kt	5

Table 2–17
U.S. Army Corps of Engineers—relative value of recreation

Annual visitors	Value rating factor
Less than 250,000	1
Greater than or equal to 250,000 but less than 1 million	2
Greater than or equal to 1 million but less than 2 million	3
Greater than or equal to 2 million but less than 4 million	4
Greater than or equal to 4 million	5

Table 2–18
U.S. Army Corps of Engineers—relative value of total economic impacts

Total economic impacts value	Value rating factor
Less than $1 million	1
Greater than or equal to $1 million but less than $100 million	2
Greater than or equal to $100 million but less than $500 million	3
Greater than or equal to $500 million but less than $1 billion	4
Greater than or equal to $1 billion	5

Table 2–19
Resource replaceability for U.S. Army Corps of Engineers Civil Works project resource

Replacement time	Value rating factor
Can be replaced within 30 days.	0
Can be replaced within 31 to 90 days.	1
Can be replaced within 91 to 180 days.	2
Can be replaced within 181 to 365 days.	3
Can be replaced within more than 365 days.	4
Possession by other than the user would harm U.S. interests far beyond the immediate user, or the	5

Table 2–19
Resource replaceability for U.S. Army Corps of Engineers Civil Works project resource—Continued

Replacement time	Value rating factor
resource cannot be replaced.	

2–4. Establishing resource value rating

Establish the value rating for resources using the results of evaluating the individual value rating factors. Sum the numerical values associated with the four applicable factors (Army mission criticality, user mission criticality, replaceability, and relative value) and compare the sum to the ranges of sums in table 2–20. Select a resultant value rating of VL, L, M, H, or VH. Enter the applicable sum and value rating in the spaces provided on DA Form 7278. Continue this procedure by proceeding to chapter 3.

Table 2–20
Resource value rating

Sum of value rating factors	Value rating
0 to 4	Very low (VL)
5 to 8	Low (L)
9 to 12	Medium (M)
13 to 16	High (H)
17 to 20	Very high (VH)

Chapter 3
Likelihood Determination

3–1. Measurement of likelihood

a. The likelihood that a given aggressor will attempt to compromise a resource is evaluated using the likelihood rating factors below. These factors measure the value of the resource to the aggressor. The first three factors are—

(1) Resource profile.
(2) Resource usefulness to aggressor.
(3) Resource availability.

b. The second three factors measure the history of or potential for incidents. These factors are—

(1) Local incidents in the past.
(2) Nearby incidents in the past.
(3) Potential for future incidents.

(4) The last three factors measure the vulnerability of the resource. These factors are weighted to emphasize vulnerability because usually only the vulnerability of a resource can be changed through security measures. The value of the resource to an aggressor and the history of or potential for incidents are difficult to control. Weighing the likelihood factors related to vulnerability allows the user of this procedure to decrease the risk level through applying security measures. These vulnerability factors are resource accessibility, effectiveness of law enforcement, and deterrence.

3–2. Evaluation procedure

Use table 3–1 to determine the aggressors that have the potential to be a threat to the resource. Eliminate those that are known not to be a threat at the location being analyzed. Enter a check mark for each applicable aggressor in the spaces provided on DA Form 7278.

Table 3–1
Potential aggressors selection table

Resource category	Unsophisticated criminals	Sophisticated criminals	Organized criminal groups	Domestic terrorists	International terrorists	State sponsored terrorists	Insider
A. Aircraft and components including unmanned aircraft systems.	X	X	X	X	X	X	X
B. Vehicles and carriage–mounted or towed weapon systems.	X	X	X	X	X	X	X
C. Communications and electronics equipment, forward repair systems, standard automotive tool sets, night vision devices and other high value optical devices, high-value precision equipment, and launched electrode stun devices	X	X	X				X
D. Organizational clothing and individual equipment	X	X	X	X	X		X
E. Subsistence items	X	X	X				X
F. Repair parts	X	X	X				
G. Petroleum, oils, and lubricants	X	X	X	X	X	X	X
H. Facility engineering supply, construction material storage areas, and industrial and utility equipment	X	X	X	X	X	X	X
I. Audiovisual equipment, training devices, and sub- caliber devices	X	X	X				X
J. Controlled cryptographic equipment	X	X	X	X	X	X	X
K. On-post public and privatized utilities	X	X	X	X	X	X	X
L. Air items and airdrop systems, and personnel and cargo parachute systems including associated ancillary items	X	X	X				X
M. USACE CW project resources	X	X	X	X	X	X	X

Table 3–1
Potential aggressors selection table—Continued

Resource category	Unsophisticated criminals	Sophisticated criminals	Organized criminal groups	Domestic terrorists	International terrorists	State sponsored terrorists	Insider
N. AA&E	X	X	X	X	X	X	X
O. Medical and medical research resources	X	X	X				X

Table 3–2
Potential likelihood rating factor table

Resource	Applicable table numbers					
A. Aircraft and components including unmanned aircraft systems.	3–3 3–9	3–4 3–10	3–5 3–11	3–6 3–15	3–7 3–16 or 3–17	3–8
B. Vehicles and carriage–mounted or towed weapon systems.	3–3 3–9	3–4 3–10	3–5 3–11	3–6 3–15	3–7 3–16 or 3–17	3–8
C. Communications and electronics equipment, forward repair systems, standard automotive tool sets, night vision devices and other high value optical devices, high-value precision equipment, and launched electrode stun devices.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
D. Organizational clothing and individual equipment.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
E. Subsistence items.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
F. Repair parts.	3–3 3–9	3–4 3–10	3–5 3–134	3–6 3–15	3–7 3–17	3–8
G. Petroleum, oils, and lubricants.	3–3 3–9	3–4 3–10	3–5 3–12	3–6 3–15	3–7 3–16	3–8
H. Facility engineering supply, construction material storage areas, and industrial and utility equipment.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–16	3–8
I. Audiovisual equipment, training devices, and sub-caliber devices.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
J. Controlled cryptographic items.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
K. On-post public and privatized utilities.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–16	3–8
L. Air items and airdrop systems, and personnel and cargo parachute systems including associated ancillary items.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
M. USACE CW project resources.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8
N. AA&E.	3–3 3–9	3–4 3–10	3–5 3–13	3–6 3–15	3–7 3–16	3–8
O. Medical and medical research resources.	3–3 3–9	3–4 3–10	3–5 3–14	3–6 3–15	3–7 3–17	3–8

3–3. Likelihood rating factors

a. Resource profile. This factor addresses the public's likely awareness of the resource's existence and its visibility to them in terms of their perception of its importance or value. Evaluate this factor for each aggressor using table 3–3.

Table 3–3
Likelihood rating factors

Level of visibility	Likelihood rating factor
Very low visibility so an aggressor is probably not aware of its existence.	1
Low visibility so its existence is probably not well known to an aggressor.	2
Medium visibility so its existence is probably known to an aggressor.	3
High visibility so its existence is probably well known to aggressor.	4
Very high visibility so its existence is obvious to an aggressor.	5

b. Resource usefulness to aggressor. This factor assesses the usefulness of the resource to potential aggressors. Usefulness is measured based on the resource's cash value, its direct applicability to the aggressor's goals, or its publicity value. Apply likelihood rating tables 3–3 through 3–18 as indicated in table 3–2 or as appropriate according to the likely goals of each aggressor type toward the resource. Enter the number of the table selected in the space provided on DA Form 7278.

(1) *Usefulness for resources with cash value.* Use table 3–4 to evaluate resource usefulness where aggressors are most likely to attempt to compromise the resource because of its potential monetary value to them. Note that the numerical values differ for different aggressor types.

Table 3–4
Usefulness for resources with cash value

Resource characteristics	Likelihood rating factor
Less than $100,000, or individual resource value is less than $10,000.	1
Greater than or equal to $100,000 and less than $250,000, or individual resource value is greater than or equal to $10,000 and less than $25,000.	2
Greater than or equal to $250,000 and less than $500,000, or individual resource value is greater than or equal to $25,000 and less than $50,000.	3
Greater than or equal to $500,000 and less than $1,000,000, or individual resource value is greater than or equal to $50,000 and less than $100,000.	4
Greater than or equal to $1,000,000, or individual resource value is greater than or equal to $100,000.	5

(2) *Usefulness for resources with direct application to aggressor's goals.* Use table 3–5 to evaluate usefulness where aggressors are most likely to attempt to compromise the resource to use it directly in future activities. An example of this would be stealing arms to use them in a future terrorist act.

Table 3–5
Usefulness for resources with direct application to aggressor's goals

Level of usefulness to aggressor	Likelihood rating factor
Resource has no usefulness to minor usefulness to aggressor's immediate or future goals.	1
Resource has moderate usefulness to aggressor's immediate or future goals.	2
Resource has significant usefulness to aggressor's immediate or future goals.	3
Resource is highly useful to aggressor's immediate or future goals.	4
Resource is critical to aggressor's immediate or future goals.	5

(3) *Usefulness for resources with publicity value.* Use table 3–6 to evaluate usefulness where aggressors are most likely to attempt to compromise a resource because of the potential publicity its compromise would generate.

Table 3–6
Usefulness for resources with publicity value

Aggressor's estimation of resource's publicity value	Likelihood rating factor
Aggressor is likely to believe resource's loss would result in insignificant publicity.	1
Aggressor is likely to believe resource's loss would result in moderate publicity.	2
Aggressor is likely to believe resource's loss would result in significant publicity.	3
Aggressor is likely to believe resource's loss would result in considerable publicity.	4
Aggressor is likely to believe resource's loss would result in worldwide publicity.	5

(4) *Resource availability.* This factor addresses the availability of the resource or similar resources at places other than in the inspectable area under consideration. Evaluate this factor for each aggressor using table 3–7.

Table 3–7
Resource availability

Determination of availability	Likelihood rating factor
Resource is widely available off the installation or site.	1
Resource has limited availability off the installation or site.	2
Resource is widely available on the installation or site, but is not available off the installation or site.	3
Resource has limited availability on the installation or site, but is not available off the installation or site.	4
Resource is only available at this location on or off the installation or site.	5

(5) *Local incidents in the past.* This factor addresses the history of attempts by the applicable aggressor to compromise similar resources at the installation or site where the resource is located or in the immediate vicinity. Evaluate this factor for each aggressor using table 3–8.

Table 3–8
Local incidents in the past

Number of incidents at the same installation or site in the past	Likelihood rating factor
There were no incidents involving similar resources on this installation or in its immediate vicinity in the past 3 years.	1
There was one incident involving similar resources on this installation or in its immediate vicinity in the past 3 years.	2
There were two or three incidents involving similar resources on this installation or in its immediate vicinity in the past 3 years.	3
There were four or five incidents involving similar resources on this installation or in its immediate vicinity in the past 3 years.	4
There were five incidents involving similar resources at this installation or in its immediate vicinity in the past 3 years.	5

(6) *Nearby incidents in the past.* This factor addresses the history of attempts by the applicable aggressor to compromise similar resources on or around other installations or sites in the same general geographic area where the resource is located. Establish the general geographic area as appropriate. Use national boundaries to determine geographic areas outside the continental United States. Evaluate this factor for each aggressor using table 3–9.

Table 3–9
Nearby incidents in the past

Number of incidents in the same geographic area in the past	Likelihood rating factor
There were no incidents involving similar resources on or around installations or sites in the geographic	1

Table 3–9
Nearby incidents in the past—Continued

Number of incidents in the same geographic area in the past	Likelihood rating factor
area in the past 3 years.	
There was one incident involving similar resources on or around installations or sites in the geographic area in the past 3 years.	2
There were two or three incidents involving similar resources on or around installations or sites in the geographic area in the past 3 years.	3
There were four or five incidents involving similar resources on or around installations or sites in the geographic area in the past 3 years.	4
There were more than five incidents involving similar resources on or around installations or sites in the geographic area in the past 3 years.	5

(7) *Potential for future incidents.* This factor addresses the probability that aggressors will attempt to compromise the resource in the future. Evaluate this factor for each aggressor using table 3–10.

Table 3–10
Potential for future incidents

Determination of probability for future incidents	Likelihood rating factor
It is unlikely there will be any future incidents involving this resource on this installation or site.	1
There is some possibility there will be a future incident involving this resource at this installation or site.	2
It is probable there will be a future incident involving this resource at this installation or site.	3
It is likely there will be a future incident involving this resource at this installation or site.	4
It is very likely there will be a future incident involving this resource at this installation or site.	5

(8) *Resource accessibility.* This factor addresses any protective measures which are in place for existing facilities or planned for new facilities. Accessibility is assessed differently depending on the resource category and either how the resources are usually stored or upon the effectiveness of protective layers. Where referenced, installing Intrusion Detection Systems (IDS) to facilitate detection is accomplished by detecting the aggressor outside the barriers that provide delay. Lightweight construction refers to construction other than reinforced concrete or masonry (concrete block or clay brick) such as wood or metal siding. Apply likelihood rating tables 3–11 through 3–17 as indicated in table 3–2. Enter the number of the selected table in the space provided on DA Form 7278.

Table 3–11
Accessibility of aircraft and vehicles

Type of storage area	Likelihood rating factor
Aircraft or vehicles are stored within locked hangars or garages with IDS or on–site guards, a perimeter fence or wall, and security lighting.	1
Aircraft or vehicles are stored within a fenced or walled area with security lighting and IDS or on–site guards.	1
Aircraft or vehicles are not stored within a fenced or walled area but are guarded by on–site guards.	2
Aircraft or vehicles are stored within a fenced or walled area with security lighting. Roving patrols check the area hourly.	2
Aircraft or vehicles are stored within a fenced or walled area with security lighting.	3
Aircraft or vehicles are stored within a fenced or walled area.	4
Aircraft or vehicles are not stored within a fenced or walled area and have no on– site guards.	5

Table 3–12
Accessibility of petroleum, oils, and lubricants and resources in outside storage areas

Type of storage area	Likelihood rating factor
Storage is within a fenced or walled area with security lighting and IDS or on–site guards.	1
Storage is within a fenced or walled area with security lighting. Roving patrols check the area hourly.	2
Storage is within a fenced or walled area with security lighting.	3
Storage is within a fenced or walled area.	4
Storage is not fenced or walled.	5

Table 3–13
Accessibility of other arms, ammunition, and explosives inside facilities

Type of storage area	Likelihood rating factor
Resource is located within multiple protective layers capable of providing delay. One of the protective layers is a safe or vault. IDS is installed to facilitate delay after detection or there is an on–site guard.	1
Resource is located within multiple protective layers capable of providing delay. IDS is installed to facilitate delay after detection or there is an on–site guard.	2
Resource is located within only one protective layer capable of providing delay and is monitored by IDS or an on–site guard.	3
Resource is located within only one protective layer capable of providing delay. The facility is checked hourly by a roving patrol.	4
Resource is located within only one protective layer capable of providing delay.	5

Table 3–14
Accessibility of resources subject to destruction, death, or injury

Type of storage area	Likelihood rating factor
Resource is located within the interior of a reinforced concrete or masonry building within a fenced or walled area with perimeter IDS or on–site guards.	1
Resource is located within the interior of a reinforced concrete or masonry building within a fenced or walled area.	2
Resource is located within a reinforced concrete or masonry building.	3
Resource is located within a building of lightweight construction.	4
Resource is located within a fenced or walled area.	5

(9) *Effectiveness of law enforcement.* This factor addresses the general attitude of the local populace regarding their respect for and cooperation with the law enforcement community and the effectiveness of local law enforcement. Effectiveness of law enforcement includes the quality of law enforcement personnel and the presence of an effective response force. Evaluate this factor for each aggressor using table 3–15.

Table 3–15
Effectiveness of law enforcement

Perceived regard for law enforcement	Likelihood rating factor
Law enforcement is extremely effective. Local populace has very high respect for law and police.	1
Law enforcement is highly effective. Local populace has high respect for law and police.	2
Law enforcement is moderately effective. Local populace has moderate respect for law and police.	3
Law enforcement is mostly ineffective. Local populace has low respect for law and police.	4

Table 3–15
Effectiveness of law enforcement—Continued

Perceived regard for law enforcement	Likelihood rating factor
Law enforcement is ineffective. Local populace has very little respect for law and police.	5

(10) *Deterrence.* This factor addresses the aggressors' perception of the possibility that they will successfully compromise the resource and escape based upon obvious protective measures which tend to have a deterrent effect. Use table 3–16 or 3–17 for each aggressor as indicated in table 3–2 or depending upon whether the resource is stored outside or inside. Enter the number of the table selected in the space provided on DA Form 7278.

Table 3–16
Deterrence for aircraft, vehicles, petroleum, oils, and lubricants, and resources in outside storage

Aggressor's perception of the possibility of success	Likelihood rating factor
Aggressor would perceive a very low possibility of success and escape. Resource appears to be heavily protected. Resource is stored within a storage structure. Obvious protective measures include fencing or a perimeter wall, security lighting, access control, and either guards or IDS and closed circuit television (CCTV).	1
Aggressor would perceive a low possibility of success and escape. Resource appears to be well protected. Obvious protective measures include fencing or a perimeter wall, security lighting, access control, and either guards or IDS and CCTV.	2
Aggressor would perceive a medium possibility of success and escape. There are some visible protective measures, including fencing or a perimeter wall, security lighting, and guard patrols at hourly intervals.	3
Aggressor would perceive a high possibility of success and escape. There are few visible protective measures. Storage area is fenced or walled.	4
Aggressor would perceive a very high possibility of success and escape. There are no visible protective measures.	5

Table 3–17
Deterrence for resources stored inside facilities

Aggressor's perception of the possibility of success	Likelihood rating factor
Aggressor would perceive a very low possibility of success and escape. Resource appears to be heavily protected. The structure housing the resource is constructed of reinforced concrete or masonry. It has window barriers or is windowless, and has heavy steel doors. Obvious protective measures include fencing or a perimeter wall, security lighting, access control, and guards or IDS and CCTV.	1
Aggressor would perceive a low possibility of success and escape. Resource appears to be well protected. The structure housing the resource is constructed of reinforced concrete or masonry. It has window barriers or is windowless, and has heavy steel doors. Obvious protective measures include fencing or a perimeter wall, security lighting, and IDS.	2
Aggressor would perceive a moderate possibility of success and escape. The structure housing the resource is constructed of reinforced concrete or masonry. It has window barriers or is windowless, and has heavy steel doors. There are some visible protective measures, including exterior lighting and hourly guard patrols.	3
Aggressor would perceive a high possibility of success and escape. The structure housing the resource is of lightweight construction and has window barriers or is windowless. There are few visible protective measures. Only structure entrances are lit.	4
Aggressor would perceive a very high possibility of success and escape. The structure housing the resource is of lightweight construction without window barriers. There are no visible protective measures.	5

3–4. Establishing likelihood rating

a. Establish the likelihood rating for each aggressor using the results of evaluating the individual likelihood rating factors.

b. Determine the highest likelihood ratings among the aggressors. Enter the likelihood ratings in the spaces provided on DA Form 7278 and compare the sum to the ranges of sums in table 3–18. Return to step 5 as discussed in paragraph 2–4 to complete this procedure.

Table 3–18
Likelihood rating

Sum of likelihood rating factors	Likelihood rating
1 to 11	Very low (VL)
12 to 22	Low (L)
23 to 33	Medium (M)
34 to 44	High (H)
45 to 55	Very high (VH)

Appendix A

References

Section I

Required Publications

AR 190–51
Security of Unclassified Army Resources (Sensitive and Nonsensitive) (Cited on title page.)

Section II

Related Publications

AR 25–30
Army Publishing Program

AR 190–11
Physical Security of Arms, Ammunition, and Explosives

AR 190–13
The Army Physical Security Program

AR 381–12
Threat Awareness and Reporting Program

JP 1–02
DOD Dictionary of Military and Associated Terms

UFC 4–020–01
DOD Security Engineering Facilities Planning Manual

Section III

Prescribed Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil).

DA Form 7278
Risk Level Worksheet (Prescribed in para 2–1.)

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil).

DA Form 2028
Recommended Changes to Publications and Blank Forms

Glossary

Section I

Abbreviations

AA&E
arms, ammunition, and explosives

AR
Army regulation

CCTV
closed circuit television

CW
Civil Works

DA Form
Department of the Army form

H
high

IDS
Intrusion Detection System

JP
Joint publication

L
low

M
medium

MW
megawatt

UFC
Unified Facilities Criteria

USACE
U.S. Army Corps of Engineers

VH
very high

VL
very low

Section II

Terms

Aggressor
Any person seeking to compromise a resource. Aggressor categories include criminals, terrorists, and protestors.

Ammunition
A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame, for use in connection with defense or offense, including demolition. Excluded from this definition are devices charged with chemical agents defined in JP 1–02 and nuclear or biological materiel. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition, and caliber .22 ammunition are excluded.

Arms
A weapon included in AR 190–11 that will or is designated to expel a projectile or flame by the action of the explosive, and the frame or receiver of any such weapon.

Controlled cryptographic item
A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but is controlled.

Criminal
A person who has committed a crime.

Critical communications facility
A communications facility that is essential to the continuity of operations of the National Command Authority during the initial phases of national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

Cryptographic component
The embodiment of a cryptographic logic in either hardware or firmware form, such as a modular assembly, a printed circuit board, a microcircuit, or any combination of these.

Cryptographic equipment
Any equipment employing a cryptographic logic.

Cryptographic logic
A deterministic logic by which information may be converted to an unintelligible form and reconverted to an intelligible form. Logic may take the form of engineering drawings, schematics, hardware, or firmware circuitry.

Domestic terrorist
Domestic terrorism involves violence against the civilian population or infrastructure of a nation—often but not always by citizens of that nation and often with the intent to intimidate, coerce, or influence national policy.

Guard
Individuals charged with performing the primary task of safeguarding designated facilities, material, and personnel within a defined area during a tour of duty. A guard may perform this function as a static post. He or she remains within or on the perimeter of a protected area and maintains continuous surveillance over that which is being protected during the tour of duty.

Insider threat
A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces. (AR 381–12).

International terrorism
Terrorism practiced in a foreign country by terrorists who are not native to that country act of terrorism, terrorism, terrorist act the calculated use of violence (or the threat of violence) against civilians in order to attain goals that are political or religious or ideological in nature; this is done through intimidation or coercion or instilling fear.

Intrusion Detection System
The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system and reporting directly to an alarm monitoring station.

Organized criminal
A category of transnational, national, or local groupings of highly centralized enterprises run by criminals who intend to engage in illegal activity, most commonly for money and profit. Some criminal organizations, such as terrorist groups, are politically motivated. Sometimes criminal organizations force people to do business with them, such as when a gang extorts money from shopkeepers for so-called "protection". Gangs may become disciplined enough to be considered organized.

Resource
Any asset requiring protection.

Risk
The degree or likelihood of loss of a resource. Factors that determine risk are the value of the resource to its user in terms of mission criticality, replaceability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the resource to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the resource.

Risk analysis
Method of examining various risk factors to determine the risk value of likelihood of resource loss. This analysis will be used to decide the level of security warranted for protection of resources.

Risk factors
Elements that make up the total degree of resource loss liability. Factors to be considered in a risk analysis include the importance of the resource to mission accomplishment; the cost, volume, criticality, and vulnerabilities of the resources; and the severity of threats to the resources.

Risk level
An indication of the degree of risk associated with a resource based on risk analysis. Risk levels may be levels I, II, or III, which correspond to L, M, and H.

Risk value
A degree of expectation or likelihood of resource loss. The value may be classified as L, M, or H for the purpose of this publication.

Sophisticated criminal
A criminal who has the ability to commit a crime to a high degree of complexity that may require planning or tools.

Unsophisticated criminal
A criminal who commits a crime which is not complicated or highly developed and does not require a high degree of complexity, planning, or tools.