Southern New Hampshire University

CJ 467 Final Project Guidelines and Rubric

Overview

In order to effectively protect public safety, criminal justice professionals need to be able to identify, prepare for, and respond to a variety of existing and potential threats. Throughout the course, we have focused on the tools and strategies that will help you perform those functions, including how to use available intelligence to assess whether and what type of threat exists, the types of resources that can be cultivated to prepare for and respond to threats, the challenges involved in sharing information and coordinating responses with others, reporting mechanisms, and response tactics once a crisis has arisen.

For the final assessment, you will imagine you are a criminal justice professional and apply the tools and techniques you have learned in the course to a specific scenario. Your task is to produce a polished report based on Suspicious Activity Reports (SARs) that have come to your attention from different sources. The report that you produce will eventually be forwarded to an appropriate agency for additional follow-up, and your goal is to facilitate that follow-up by succinctly communicating what you know about the possible threat and what can be done to mitigate it. Your finished intelligence report should identify the type of adversary, ascertain the appropriate agency for eventual follow-up activities, assess the threat level (using an intelligence threat scale), and suggest countermeasures and information protection actions needed to address the threat.

The project is divided into **two milestones**, which will be submitted at various points throughout the course to scaffold learning and ensure quality final submissions. These milestones will be submitted in **Modules Three and Five.** The final product will be submitted in **Module Seven.**

In this assignment, you will demonstrate your mastery of the following course outcomes:

- CJ-467-01: Formulate strategies for combating threats within the criminal justice professional's scope of responsibility by analyzing the types of adversaries law enforcement officers may encounter
- CJ-467-02: Analyze law enforcement and the intelligence community's perceptions of threat for briefing the appropriate agency
- CJ-467-03: Assess the opportunity, capability, and intent of known adversaries and the vulnerability of potential targets in constructing appropriate threat scales for scenarios that criminal justice professionals might face
- CJ-467-04: Assess the vulnerability of critical information related to potential targets and law enforcement activities by applying the operations security process

Prompt

Imagine that you are a member of a law enforcement agency and you have received several pieces of raw intelligence from different sources (Suspicious Activities Reports or SARs), which, when taken together, point to a potential threat from a specific adversary. The SARs can be found in the Assignment Guidelines and Rubrics section of the course.

Your job is to create a clear and comprehensive report that analyzes the intelligence from the SARs in order to pass it on to the appropriate agency. You should structure your report so that the agency, in turn, can respond to the threat in a way that is effective and appropriate given what you have learned. The finished

report should sort the information chronologically, funnel it down to a specific adversary, identify the potential target(s) for the adversary's activities, assess the level of threat, and make suggestions about what can be done to counter the threat and protect critical information so that the adversary does not change the target. Because most intelligence is fragmented, you will need to read all of the SARs carefully in order to gather the necessary information for the finished intelligence report. Remember to use direct language and employ criminal justice terminology appropriate for the type of threat being assessed and the receiving agency. Accuracy and appropriate grammar are also essential for the report's credibility.

Specifically, the following **critical elements** must be addressed:

I. **Executive Summary**

In this section, you should accurately highlight the essential elements of the intelligence report for quick reference by the agency receiving the report. You should include the name of referring agent (your name), the name of the agency that you are imagining you work for, the current date, dates of the activities being covered in the intelligence report, and a brief summary (two to three sentences) on the adversary, scope, and nature of the potential threat. Although this is the opening section of the report, you may wish to complete it last in order to accurately capture the analysis of the body of your report.

II. **Adversary, Motivation, and Jurisdiction**

This section starts with a consolidated summary of the Suspicious Activity Reports (SARs) provided, and covers who may be planning to carry out criminal activities, their motivations, and under whose jurisdiction the activities fall.

A. Accurately **summarize** the intelligence collected from the SARs to date, focusing on the "who, what, when, where, why, and how" of the threat situation. Information should be annotated with dates and times from relevant SARs, and information from each date should be provided in a separate paragraph, from inception to most recent. Your summary should focus on connecting the dots, with as much detail as needed to present all the relevant intelligence. It should highlight information that would be of particular relevance for the law enforcement agency doing follow-up in understanding the potential threat.

B. Determine who the **adversary** is for this potential threat. It may be an individual or a group. You should identify the names of suspects (if known) and also the type of adversary. For example, is the adversary an international terrorist group, a domestic terrorist group, an organized crime, a local or international gang, drug traffickers, an extremist or militia group, a hacker, or a white-collar criminal? Support your answer using relevant information from the SARs.

C. Analyze the **range** of the adversary's operations. Are their activities focused within one city or state or across multiple states? Support your answer with relevant information from the SARs.

D. Analyze what is known about the adversary's **motivation** and how that might affect their choice of target (individual or location). Might it affect whether they choose one target or many, the type of target they select, or the location of the attack? Support your answer with relevant information from the SARs.

E. Based on your analyses in Parts A–C above, determine which agency has **jurisdiction** in following up on the potential threat. For example, should local or state law enforcement follow up? Should federal law enforcement? Does the adversary's choice of potential targets fall under a particular jurisdiction? For example, threats to air travel might involve the FAA or TSA, while terrorist threats would go to the FBI. Be sure to justify your answer using relevant information from the SARs.

III. **Threat Assessment**

In this section of the report, you should lay out what is known about the nature and imminence of the potential threat. You may wish to use the Threat Assessment Worksheet, found in the Assignment Guidelines and Rubrics section of the course, to record and analyze relevant information from Suspicious Activities Reports (SARs) in preparing your response. However, you should present the information from the worksheet in narrative form in your finished intelligence report.

A. Distinguish the **nature** of the threat, including specific potential target(s), the location of likely attack (if the target is an individual), and potential means of attack based on the summary information and analysis above. Draw out the elements that would be most important to the agency receiving the report in determining the threat and focusing their efforts.
B. Assess whether the adversary has the **intent**, opportunity, and capability to carry out a threatening behavior. Is the threat being actively pursued? Support your answer with information from the SARs.
C. Assess the **vulnerabilities** of the potential target(s) and law enforcement's ability to protect the target(s). Support your answer using information from the SARs and reasonable assumptions about potential vulnerabilities. For example, how tight is security for entry into a particular building? Could a target be threatened from a street location? Could law enforcement be impeded from quickly responding to a threat? Note that these questions are illustrative only, and the vulnerabilities that you identify should correspond to your analysis of the specific threat identified.
D. Using the analyses in Parts A–C above, assess the **current level of risk** using a scale from 0–10, with 0 being "no threat" and 10 being "great threat." How imminent is the threat? Is it going to happen now, next week, in the next year, never? What level of damage could the adversary inflict if they are successful in carrying out the threat? Justify your answer based on your analysis.
E. Recommend what **countermeasures**, if any, might be appropriate for addressing vulnerabilities and mitigating the potential threat that you identified above. Depending on your analysis, you may suggest multiple countermeasures, a single countermeasure, or no countermeasures. Be sure to support your answer using your threat assessment analysis and information from the SARs.

IV. **Information Security**

In this section of the report, you should address how to protect critical information from falling into the hands of the adversary (i.e., operations security). You may wish to use the Operations Security Worksheet, found in the Assignment Guidelines and Rubrics section of the course, to record and analyze relevant information from the Suspicious Activity Reports (SARs) in preparing your response. However, you should present the information from the worksheet in narrative form in your finished intelligence report.

A. Assess what **critical information** surrounding the potential target and law enforcement activities to mitigate the threat needs to be protected. In other words, what information do we not want the adversary to have and why? Justify your answer.
B. Assess the **adversary's methods** for collecting intelligence about their target and law enforcement activities. Are they making multiple visits to the target? Are they using informants within the community? Are they doing research on the internet? Monitoring police bands? Taking pictures? What other methods might they be using? Support your answer using information from the SARs and reasonable assumptions.

C. Assess **potential weaknesses** in information security that might give away critical details about the target or law enforcement activities. Support your answer using information from the SARs and reasonable assumptions.
D. **Risk assessment.** Using the analyses in Parts A–C above, assess the current level of risk from information security weaknesses as high, medium, or low. In other words, how high is the risk that the adversary will obtain the critical information, and what level of damage could the adversary inflict if the information is acquired? Support your answer using information from the SARs and reasonable assumptions.
E. **Recommendations.** Suggest what countermeasures, if any, might be appropriate for addressing the information security vulnerabilities you identify above. Justify these suggestions in terms of monetary cost versus effectiveness. How can we prevent or subvert the adversary's methods for collecting intelligence? How do we keep the adversary from knowing that we are aware of the threat and acting to avert it? Depending on your analysis, you may recommend multiple countermeasures, a single countermeasure, or no countermeasures. Be sure to support your answer using your operations security analysis and information from the SARs.

Milestones

Milestone One: *Report*
In **Module Three**, using the Suspicious Activity Reports (reports #1–16), analyze and describe the elements of adversary, range, motivation, and jurisdiction of the population. **This milestone will be graded with the Milestone One Rubric.**

Milestone Two: *Threat Assessment*
In Module Five, using the Suspicious Activity Reports (reports #1–16), analyze and describe the threat assessment in the scenario given in the assignment. Include information regarding the nature of the threat, the vulnerabilities of the potential targets, current level of risk, and possible countermeasures. **This milestone will be graded with the Milestone Two Rubric.**

Final Submission: *Intelligence Report*
In **Module Seven**, you will submit your final project. It should be a complete, polished artifact containing **all** of the critical elements of the final product. It should reflect the incorporation of feedback gained throughout the course. **This submission will be graded with the Final Project Rubric.**

Final Project Rubric

Guidelines for Submission: Your finished intelligence report should be 5–10 pages in length with double spacing, 12-point Times New Roman font. Remember to write the finished intelligence report in third person and in chronological order. You should also attach a copy of the Suspicious Activity Reports (SARs) as an appendix to your proposal. Although this is not a graded component of the assessment, including it in the appendix provides the agency receiving the report with additional detail and supporting documentation.

Southern New Hampshire University

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Executive Summary	Meets "Proficient" criteria and executive summary models real-world language, style, and brevity	Accurately highlights essential elements of the intelligence report for quick reference by the agency receiving the report	Highlights essential elements of the intelligence report, but key information is missing or inaccurate	Does not highlight essential elements of the intelligence report	6
Adversary, Motivation, and Jurisdiction: Summarize	Meets "Proficient" criteria and summary is exceptionally articulate, modeling language that would be used in a real-world intelligence report and expertly balancing detail with brevity and clarity	Accurately summarizes intelligence collected to date, in chronological order from inception to most recent, with date and time annotations from relevant SARs, highlighting all relevant information for the agency doing follow-up in understanding potential threat	Summarizes intelligence collected to date, but summary is inaccurate, incomplete, not presented in chronological order with date and time annotations, or does not highlight information of particular relevance for the law enforcement agency doing follow-up	Does not summarize the intelligence collected to date	6
Adversary, Motivation, and Jurisdiction: Adversary	Meets "Proficient" criteria and answer is particularly well supported, expertly balancing detail with brevity and clarity	Determines adversary for this potential threat, including suspect names (if known) and type of adversary, supported by relevant information from the SARs	Determines who the adversary is and adversary type, but determination is not supported by relevant information from the SARs	Does not determine who the adversary is and adversary type	6
Adversary, Motivation, and Jurisdiction: Range	Meets "Proficient" criteria and response identifies specific locations as well as whether they are confined to a particular city, state, or multiple states	Analyzes adversary's range of operations, supported by relevant information from the SARs	Analyzes adversary's range of operations, but analysis is not supported by relevant information from the SARs	Does not analyze adversary's range of operations	6
Adversary, Motivation, and Jurisdiction: Motivation	Meets "Proficient" criteria and analysis shows insight into how adversary's motivations affect elements of the threat beyond the choice of target	Analyzes adversary's motivation and how that might affect their choice of target, supported by relevant information from the SARs	Analyzes adversary's motivation and how that might affect their choice of target, but analysis is not supported by relevant information from the SARs	Does not analyze adversary's motivation and how that might affect their choice of target	6

Adversary, Motivation, and Jurisdiction: Jurisdiction	Meets "Proficient" criteria and answer considers how jurisdictional responsibilities may overlap or affect operations related to the specific threat scenario	Determines which agency has jurisdiction in following up on the potential threat, supported by analysis of adversary and relevant information from the SARs	Determines which agency has jurisdiction in following up on the potential threat, but does not support using analysis of adversary and relevant information from the SARs	Does not determine which agency has jurisdiction in following up on the potential threat	6
Threat Assessment: Nature	Meets "Proficient" criteria and analysis is exceptionally articulate, modeling language that would be used in a real-world intelligence report and expertly balancing detail with brevity and clarity	Distinguishes the nature of the threat, including specific target(s), location (if target is an individual), and potential means of attack based on analysis of SARs, emphasizing elements that would be most important to the agency receiving the report in determining the threat and focusing their efforts	Distinguishes the nature of the threat based on analysis of SARs, but does not emphasize elements that would be most important to the agency receiving the report	Does not distinguish the nature of the threat based on analysis of SARs	6
Threat Assessment: Intent	Meets "Proficient" criteria and assessment is exceptionally articulate, modeling language that would be used in a real-world intelligence report and expertly balancing detail with brevity and clarity	Assesses whether adversary has the intent, opportunity, and capability to carry out a threatening behavior and whether threat is being actively pursued, supported by relevant information from the SARs	Assesses whether adversary has intent, opportunity, and capability to carry out a threatening behavior and whether threat is being actively pursued, but assessment is not supported by relevant information from the SARs	Does not assess whether adversary has intent, opportunity, and capability to carry out a threatening behavior or whether threat is being actively pursued	6
Threat Assessment: Vulnerabilities	Meets "Proficient" criteria and analysis addresses a broad spectrum of vulnerabilities surrounding the potential target and law enforcement activities in this threat scenario	Analyzes vulnerabilities of the potential target(s) and law enforcement's ability to protect the target(s), supported by information from the SARs and reasonable assumptions	Analyzes vulnerabilities of potential target(s) and law enforcement's ability to protect target(s), but analysis is not supported by information from SARs and reasonable assumptions	Does not analyze vulnerabilities of the potential target(s) or law enforcement's ability to protect the target(s)	6
Threat Assessment: Current Level of Risk	Meets "Proficient" criteria and analysis of imminence and potential damage is particularly well supported	Assesses the current level of risk, including imminence and potential damage, using a scale from 0–10, and justifies rating based on analysis of SARs	Assesses current level of risk, including imminence and potential damage, using a scale from 0–10, but does not justify rating based on analysis of SARs	Does not assess current level of risk, including imminence and potential damage, using a scale from 0–10	6

Treat Assessment: Countermeasures	Meets "Proficient" criteria and recommendations are particularly well aligned with specific needs of the scenario and real–world constraints	Recommends what countermeasures, if any, might be appropriate for addressing vulnerabilities and mitigating the threat identified, supported by threat assessment analysis and information from the SARs	Recommends what countermeasures, if any, might be appropriate, but recommendations are not supported by threat assessment analysis and information from the SARs	Does not recommend what countermeasures, if any, might be appropriate for addressing vulnerabilities and mitigating the threat	6
Information Security: Critical Information	Meets "Proficient" criteria and justification is particularly well supported	Assesses what critical information surrounding the potential target and law enforcement activities to mitigate the threat needs to be protected, and justifies response	Assesses what critical information needs to be protected, but does not justify response	Does not assess what critical information needs to be protected	6
Information Security: Adversary's Methods	Meets "Proficient" criteria and assessment addresses a broad and realistic spectrum of methods given the parameters of this threat scenario	Assesses the adversary's methods for collecting intelligence about target and law enforcement activities and supports answer using information from SARs and reasonable assumptions	Assesses adversary's methods for collecting intelligence, but does not support answer using information from SARs and reasonable assumptions	Does not assess adversary's methods for collecting intelligence	6
Information Security: Potential Weaknesses	Meets "Proficient" criteria and assessment addresses a broad and realistic spectrum of potential information security weaknesses given the parameters this threat scenario	Assesses potential weaknesses in information security, and supports answer using information from the SARs and reasonable assumptions	Assesses potential weaknesses in information security, but does not support answer using information from the SARs and reasonable assumptions	Does not assess potential weaknesses in information security	6

Information Security: Risk Assessment	Meets "Proficient" criteria and assessment of likelihood of breach and potential damage are particularly well supported	Assesses the current level of risk from information security weaknesses, including likelihood of adversary obtaining information and the damage that could be inflicted, using a high-medium-low scale, and supports assessment with information from SARs and reasonable assumptions	Assesses the current level of risk from information security weaknesses, using a high-medium-low scale, but does not support with information from SARs and reasonable assumptions	Does not assess the current level of risk from information security weaknesses	6
Information Security: Recommendations	Meets "Proficient" criteria and suggestions are particularly well aligned with the specific needs of the scenario and real-world constraints	Suggests what countermeasures, if any, might be appropriate for addressing information security vulnerabilities, supported by operations security analysis and information from SARs	Suggests what countermeasures, if any, might be appropriate, but recommendations are not supported by operations security analysis and information from SARs	Does not suggest what countermeasures, if any, might be appropriate for addressing information security vulnerabilities	6
Articulation of Response	Submission is free of errors related to citations, grammar, spelling, syntax, and organization and is presented in a professional and easy-to-read format	Submission has no major errors related to citations, grammar, spelling, syntax, or organization	Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas	4
				Earned Total	**100%**