The Teacher Notes were developed to help teachers understand the depth and breadth of the standards. In some cases, information provided in this document goes beyond the scope of the standards and can be used for background and enrichment information. Please remember that the goal of social studies is not to have students memorize laundry lists of facts, but rather to help them understand the world around them so they can analyze issues, solve problems, think critically, and become informed citizens.

TEACHER NOTES
Introduction to U.S. Intelligence and National Security Studies

Verbatim from Standards of Excellence: *Introduction to U.S. Intelligence and National Security Studies provides a basic and broad overview of the career field of Intelligence, the authorized activities of an intelligence professional, the composition of the United States Government Intelligence Community (IC), the various functions of each of the member agencies, the limits and capabilities of Intelligence and how Intelligence plays a role in the decision-making process of the government. This course is also designed to apply critical analysis to the field of U.S. Intelligence.*

SSIUSINS1 – Examine the development of the field of U.S. Intelligence.

a. Explore the history of U.S. Intelligence efforts from the American Revolution through the Civil War.

It is imperative to debunk the common perception that the intelligence field is full of individuals like the fictional characters James Bond, Jason Bourne, Lorraine Broughton, and Ethan Hunt. Intelligence is a process (e.g., the intelligence cycle) and a product (e.g., the national intelligence estimate).

When discussing the history of the field of intelligence you will notice an ebb and flow of public and government perception of intelligence – which usually was directly related to a regional or international conflict. Key points in this history span from pre-Revolutionary War to post-9/11. *Note: The International Spy Museum in Washington, D.C. offers virtual education events which may prove useful when discussing history: https://www.spymuseum.org/education-programs/educators/interactive-virtual-field-trip/*

The history of U.S. intelligence begins with George Washington two decades before the **Revolutionary War.** Washington served as an intelligence collector while serving the British during the French and Indian War in the 1750s. Fast forward to the Revolutionary War, George Washington quickly realized that the American Continental Army could not out-power the British, so they would need decision advantage. Washington created the Secret Committee and the Committee of Secret Correspondence which reported on British troop movements and conducted covert operations. He also relied on a group of spies called the Culper Spy Ring to transport intelligence about the movements of the British. Another aspect of intelligence practiced during this time was counterintelligence (keeping valuable information out of the hands

of the enemy). The British equally understood the significance of decision advantage and one of the infamous events is the British successful recruitment of a Continental Army general named Benedict Arnold. Benedict Arnold's plan to provide information about the Continental Army's command post at West Point, New York was foiled, but it highlights the noted importance of attaining intelligence of adversary intentions and actions. Once the Revolutionary War ended, Washington did not form a permanent intelligence service in America. Instead he used intelligence as the need arose (e.g., the War of 1812 and the Mexican War of 1846).

Civil War: During the Civil War both the North and the South established intelligence operations. Military commanders used a variety of sources, in some cases civilians. One of the most notable examples is the role **Harriet Tubman** played in intelligence operations during the Civil War. In addition to leading the Underground Railroad to free slaves, she often debriefed those slaves leaving the South to gain valuable information on any confederate activity they observed. Her network of spies became known as the Black Dispatches. Another significant development during the Civil War involved collecting information using new technology.

Resources:

1. HISTORY Channel: "How George Washington Used Spies to Win the American Revolution https://www.history.com/news/george-washington-general-espionage-culper-spy-ring
2. CIA: "Black Dispatches: Black American Contributions to Union Intelligence During the Civil War" https://www.cia.gov/resources/csi/books-monographs/black-dispatches-black-american-contributions-to-union-intelligence-during-the-civil-war/
3. National Air & Space Museum: "Civil War Ballooning https://airandspace.si.edu/learn/highlighted-topics/civil-war-ballooning

SSIUSINS1 – Examine the development of the field of U.S. Intelligence.

b. Explain the application of U.S. intelligence from the World War I to World War II.

World War I: The volume of information regarding intelligence during WWI pales in comparison to the literature available regarding the use of intelligence in WWII. It is possible that the literature is sparse because the focus of intelligence leading up to and throughout WWI was domestic in nature. Government officials and entities within the United States were seemingly focused on rooting out known or perceived anarchists (individuals that shared Communist ideology) following the 1917 Russian Revolution. It may be worth reiterating this point in history when discussing law enforcement intelligence (SSIUSINS3b). But for the sake of historic significance, during the investigation of anarchists, J. Edgar Hoover served as the director of the General Intelligence Division of the Bureau of Investigation - which would later become the **Federal Bureau of Investigation** (FBI) in 1935. Between 1919 and 1920, Hoover and Attorney General Mitch Palmer led the **Palmer Raids** which received criticism by groups such as the American Civil Liberties Union (ACLU) for its unlawful investigation of people solely based on their affiliation with anarchists or socialist groups. The intelligence operations during this period also bring to bear a larger discussion of how intelligence can become

politicized. The Palmer Raids also ushered in a broader discussion of the responsibility of the U.S. intelligence community to protect the nation while safeguarding the constitutional freedoms of its citizens.

Resources:

1. FBI Archives: "A Byte out of History: The Palmer Raids" https://archives.fbi.gov/archives/news/stories/2007/december/palmer_122807
2. HISTORY Channel: "The Palmer Raids" https://www.history.com/topics/red-scare/palmer-raids

World War II: As one explores the history of U.S. intelligence, the ebb and flow of how intelligence assets and programs were properly utilized to its greatest potential is worth noting (possibly due to a lack of foresight). For example, during the course of World War I, the **Cipher Bureau** (also known as **The Black Chamber**) was established and successfully decrypted message traffic from foreign governments. However, the Cipher Bureau was disbanded in 1929 as Secretary of State Henry Stimson is famously quoted as saying "gentlemen don't read each other's mail." Historians submit that had the Cipher Bureau continued operations, it is likely operators would have been able to break the Japanese naval code and provide forewarning to the December 7, 1941 surprise attack against Pearl Harbor. Nevertheless, following the Pearl Harbor attack, the U.S. government acknowledged the dire need to improve the intelligence apparatus and the coordination among the entities.

In 1941, President Franklin D. Roosevelt created a new organization and appointed William J. Donovan as the **Coordinator of Information** (COI). The office of the COI became the first peacetime intelligence organization to provide all-source intelligence and improve integration and collaboration among agencies. As World War II continued, it became clear that the COI needed to expand, which led to the establishment of the **Office of Strategic Services** (OSS) in 1942 that was headed by William Donovan (who had earned the nickname "Wild Bill"). The OSS would become the predecessor to the Central Intelligence Agency. Some intelligence victories during World War II include: the early-1942 JN-25 code breaking which facilitated the breaking of the Japanese "Purple code," the subsequent U.S. victory in the Battle of Midway and the Battle of Coral Sea, as well as the FBI's 1942 investigation of suspected foreign spies and saboteurs, including the Nazi's Operation Pastorius ring.

Resources:

1. NSA: "The Black Chamber" https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/pearl-harbor-review/black-chamber/
2. CIA: "CIA: History of CIA" https://www.cia.gov/legacy/cia-history/
3. CIA: "CIA: The Office of Strategic Services" https://www.cia.gov/legacy/museum/exhibit/the-office-of-strategic-services-n-americas-first-intelligence-agency/
4. NSA: "A History of U.S. Communications Intelligence during World War II" https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/history_us_comms.pdf
5. HISTORY Channel: "Battle of Midway" This is a **great 15 min video**: https://www.youtube.com/watch?v=kipF5zoCGAk

- Here is another source for the Battle of Midway with a photo gallery: https://www.history.com/topics/world-war-ii/battle-of-midway.

SSIUSINS1 – Examine the development of the field of U.S. Intelligence.

c. Explain how the late and post-Cold War era shaped U.S. intelligence agencies.

Cold War: Following the 1917 revolution that led to the creation of the Soviet Union, the United States became increasingly concerned given the stark contrast between the values and ideology of Communism and capitalism. In 1943, the U.S. Army worked with British Intelligence on a Signals Intelligence (SIGINT) operations called **Project Venona** which monitored Soviet communications until 1980. This project would provide invaluable information about Soviet spy rings operating in the United States and provide insight into Soviet intentions. Likewise, it also shed light on Soviet spies, such as the **Rosenberg Spy Ring** that provided damning intelligence to the Soviets – some of which led to the development of a Soviet atomic bomb. As noted in the 1946 "Long Telegram," the United States would change tactics in dealing with the Soviets by attempting to contain their expansion. Ultimately, the **containment** strategy would drive intelligence and diplomatic efforts throughout the Cold War. The Cold War is often cited as an intelligence war given the extensive spying on each other and covert operations. It is also cited as giving birth to the U.S. intelligence infrastructure.

The **National Security Act of 1947** remains a very important piece of legislation in the U.S. intelligence community. It created the Central Intelligence Agency (CIA), the Department of Defense, and the National Security Council. It also established laws regarding intelligence collection and covert activities. Prior to the establishment of this act, President Truman (reminiscent of the OSS during World War II) did not want what would become the CIA to become too powerful of an organization. Therefore, two key elements of the NSA of 1947 restricted the CIA by (1) not giving it law enforcement powers and (2) mandating that it operates primarily outside of the United States.

The Cold War was also comprised of several proxy wars. Countries used spy tradecraft via covert activities to shape the geopolitics of the world. Some examples include the CIA's funding of Italy's opposition party, the Christian Democrats to stave growing pro-Communist sentiments in Italy's 1948 elections; **Operation Ajax** (a 1953 CIA-engineered Iranian coup to unseat Prime Minister Mohammed Mosaddeq because he threatened to nationalize oil companies in Iran that belonged to Britain); and a 1954 CIA-engineered Guatemalan coup to unseat President Jacobo Guzman who contemplated redistributing foreign wealth to his citizens. Although Operation Ajax was initially considered a success, it would later become a historic example of poor intelligence analysis and intelligence collection. Intelligence analysts (primarily within the CIA) lacked the key information to identify how Shah Mohammad Reza Pahlavi (once very popular) was rapidly losing support of the Iranian people. The growing influence of Islamic clerics was also key information that was not realized until after the revolution that unseated the Shah and led to the establishment of the Islamic Republic. Shortly after he was ousted, Iranian students breached the U.S. Embassy in Tehran and

held 52 American diplomats hostage for 444 days. It would become known as the "Iranian Hostage Crisis."

Legislation out of Disruption: Without the establishment of legislation, the U.S. intelligence apparatus was used as a tool to investigate suspected internal threats. For example, between the 1950s and the 1970s, policy makers within the U.S. government became increasingly suspicious of Communist sympathizers, the Civil Rights movement, and major protests for equality by U.S. citizens. In the 1950s, the anti-communist crusades were often coined "The Red Scare." In 1956, the FBI, under J. Edgar Hoover, began the Counterintelligence Program (**COINTELPRO**) to disrupt the known and suspected activities of the Communist Party of the United States. However, in the 1960s, it was expanded to include a number of other domestic groups, such as the Ku Klux Klan, the Socialist Workers Party, and the Black Panther Party. All COINTELPRO operations were ended in 1971. Although limited in scope, COINTELPRO was later rightfully criticized by Congress and the American people for abridging first amendment rights and for other reasons. Around the same time, in the 1960s, the CIA conducted investigations on American citizens that were suspected domestic dissidents, code named **Operation CHAOS**. The CIA was most concerned about foreign influence inside some civil-unrest movements. In the late 1960s and early '70s, that meant looking for foreign linkages to the antiwar movement, the black nationalism movement (the Black Panther Party) and civil-rights groups, such as the Southern Christian Leadership Conference.

These actions in addition to the 1972 Watergate scandal under the Nixon administration led to increased distrust of the U.S. government. As a result, two investigative committees were formed in 1975. On 27 January 1975, the US Senate established the Senate Select Committee to Study Government Operations With Respect to Intelligence Activities (the Church Committee). On 19 February 1975, the House voted to create a House Select Intelligence Committee (the Nedzi Committee, which was replaced five months later by the Pike Committee.). **The Church Committee** held a series of public hearings in September and October of 1975 to educate the American public about the "unlawful or improper conduct" of the intelligence community, highlighting a few carefully selected cases of misconduct. These hearings examined a CIA biological agents program, a White House domestic surveillance program, IRS intelligence activities, and the FBI's program to disrupt the civil rights and anti-Vietnam War movements. These nationally televised events offered the American public an opportunity to learn about the secret operations conducted for decades by U.S. intelligence agencies. **The Pike Committee** investigated whether agencies within the Intelligence Community were carrying out their duties effectively and efficiently. Due to infighting between the committee members and the CIA, the findings of the Pike Committee were never released to the public.

However, the release of findings from the Church Committee led to public outcry and the subsequent passage of the **Foreign Intelligence Surveillance Act of 1978**. This Act established judicial oversight of the U.S. government's surveillance of foreign entities within the United States. The Act also established guidelines for surveillance (electronic and physical) as well as requirements for utilizing intelligence collection resources. Due to the change in technology and methods of communication, this act was amended in 2008 - called the FISA Amendments Act (FAA) to using intelligence collection assets to acquire foreign intelligence information about the plans and identities of entities that threaten the U.S. This amendment also facilitated the

collection of U.S. persons abroad that were involved in nefarious activity targeting the U.S. government.

An important period of intelligence history is what is commonly referred to as **The Year of the Spy.** The 1985, there were a few high-profile espionage arrests by the FBI and hence the term "the Year of the Spy." Several spies arrested include Jonathan Jay Pollard (a U.S. Navy intelligence analyst spying for Israel) and three spies that were working for China, Ghana, and the Soviet Union respectively. Within this timeframe, additional investigations led to the eventual arrests of Aldrich Ames (a CIA case officer spying for the Soviet Union) and Robert Hanssen (a FBI Special Agent spying for Russia).

Another important period of intelligence history is the **impacts of terrorism** and the subsequent passing of the USA PATRIOT Act of 2001 and the Intelligence Reform and Terrorism Prevention Act of 2004. Following the fall of the Soviet Union, policy makers within the U.S. government gradually began to realize that although terrorism was not "new," it was becoming a prominent threat to U.S. national interests abroad and at home. One of the terrorist attacks that led to that realization occurred in October 1983 when the Lebanese Hezbollah terrorist group conducted a suicide attack against the U.S. Marine barracks in Beirut, Lebanon. Other terrorist attacks include: the December 1988 attack against Pan American Flight 103; the February 1993 attack against the World Trade Center in New York; the April 1995 attack against the FBI Murrah Building in Oklahoma City, Oklahoma; the August 1998 near-simultaneous attacks against the U.S. embassies in Nairobi, Kenya and Dar es Salam, Tanzania; the October 2000 attack against the USS Cole in a Yemeni port; and the September 2001attacks in the U.S.

Following the September 2001 attacks, in October 2001 President George W. Bush signed the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* **(USA PATRIOT) Act of 2001**. Among other purposes, this act was enacted to deter and punish terrorist acts in the U.S. and around the world and to enhance law enforcement investigatory tools. Among other things, this act created the Department of Homeland Security (DHS) and also strengthened the ability to detect and prosecute international money laundering and the financing of terrorism. Upon the conclusion of the 9/11 Commission and the publishing of the report, President George W. Bush signed the **Intelligence Reform and Terrorism Prevention Act of 2004** (IRTPA of 2004). This act created the Office of the Director of National Intelligence (ODNI), the National Counterterrorism Center, and the Privacy and Civil Liberties Oversight Board.

Resources:

1. NSA: "VENONA" https://www.nsa.gov/news-features/declassified-documents/venona/
2. FBI: "Atom spy case/Rosenbergs" https://www.fbi.gov/history/famous-cases/atom-spy-caserosenbergs
3. HISTORY Channel: "President Truman Signs the National Security Act" https://www.history.com/this-day-in-history/truman-signs-the-national-security-act
4. Stanford University: "Operation Ajax" https://history.stanford.edu/news/aug-19-1953-operation-ajax-priya-satia

5. HISTORY Channel: "The Iranian Hostage Crisis" https://www.history.com/this-day-in-history/iran-hostage-crisis-ends
6. FBI "COINTELPRO" https://vault.fbi.gov/cointel-pro
7. HISTORY.com "Operation CHAOS" https://www.history.com/news/cia-surveillance-operation-chaos-60s-protest
8. Senate.gov "The Church Committee" https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm
9. CIA "The Pike Committee" https://apps.dtic.mil/dtic/tr/fulltext/u2/a525280.pdf
10. ODNI, "FISA Amendments Act," https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf
11. FBI, "Year of the Spy (1985)," https://www.fbi.gov/history/famous-cases/year-of-the-spy-1985
12. FBI, Overview of terrorist attacks targeting the US: https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-confronting-the-united-states
13. ODNI, "USA PATRIOT Act," https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2116-usa-patriot-act
14. ODNI, "IRTPA Act," https://www.dni.gov/files/NCTC/documents/RelatedContent_documents/Intelligence_Reform_Act.pdf

SSIUSINS1 – Examine the development of the field of U.S. Intelligence.

d. Analyze the current challenges of the U.S. Intelligence community (e.g., social media and information warfare).

Identifying current challenges will obviously depend on the current environment (e.g., when you're preparing to teach this course). However, some common themes to consider that will likely be relevant for a longer period of time include: (1) the impacts of social media on intelligence collection; (2) the convergence of technology; and (3) impacts of influence operations and information warfare on intelligence analysis. The key takeaway regarding current challenges is that analysts, collectors, and operators in the intelligence field are working within an operational environment that is continuously evolving. The most significant and impactful challenges are described in the *Global Trends 2030: Alternative Worlds*. This document examines megatrends and game-changers that can impact U.S. intelligence activity and by extension U.S. national security interests. Note: *I recommend reviewing the Global Trends 2030 document with an emphasis on the assessed megatrends, game-changers, and the potential worlds. As noted in the document, the effects of globalization, the convergence of technology, and shortage of natural resources have secondary and tertiary effects.*
Resources: National Intelligence Council "Global Trends 2030" https://www.dni.gov/files/documents/GlobalTrends_2030.pdf

SSIUSINS2 – Describe the basic roles and functions of the Intelligence field.

a. Define Intelligence as the process of collection and analysis of information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests.

Intelligence is a dynamic concept with more than one definition that varies between organizations. For example, the FBI, the CIA, and the Department of Defense have different definitions. However, when teaching this course, the definition of intelligence provided by the Office of the Director of National Intelligence is recommended: *Intelligence is information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security. Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probably outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform official travelers of counterintelligence and security threats*. Note: periodically review the ODNI resource link below to verify the most up to date definition of intelligence.

Resource:

ODNI: "What is Intelligence" https://www.dni.gov/index.php/what-we-do/what-is-intelligence

SSIUSINS2 – Describe the basic roles and functions of the Intelligence field.

b. Explain the purpose and uses of Intelligence for the U.S. government.

When explaining the purpose and uses of intelligence, it is important to distinguish between the purpose of intelligence and the functions of intelligence – both of which are briefly highlighted in the ODNI's explanation of "what is intelligence."

Purpose: In the simplest of explanation, the purpose of intelligence is to inform the decision maker. Generally, the decision maker wants intelligence to answer three questions (intent, capability, and potential effects or ICE as an acronym to remember):

1. What (known or suspected) **capabilities** do U.S. adversaries possess?
2. What are the **intentions** of U.S. adversaries – in particular, what is the most dangerous thing they may do?
3. What **effect** might all this have on the U.S.'s ability to accomplish its national goals?

Functions: A main function of the intelligence field is to provide decision makers and policy makers (at all levels) with **decision advantage** (where one knows more than a competitor or adversary). Note*: further discussion of examples of intelligence disciplines as well as examples of intelligence victories will highlight specific examples of decision advantage.* In that same vein, there are **five functions of intelligence agencies**: collection (gathering information and data), analysis ("connecting the dots"), counterintelligence (protecting information and intelligence from people and organizations that should not have the information), covert operations

(concealed operations where the intent is to maintain plausible deniability), and intelligence management (organizing and processing data, storing information, and disseminating intelligence throughout the IC).

Resources:

1. Intel.Gov, "How the IC Works" https://www.intelligence.gov/how-the-ic-works
2. ODNI: "An Overview on the Intelligence Community (2013)" https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf

SSIUSINS2 – Describe the basic roles and functions of the Intelligence field.

c. Describe the various career paths for a person entering the Intelligence field (e.g., analytical, operational, and technical).

When explaining the various career paths for a person entering the intelligence field, it is first important to explain the members of the Intelligence Community (IC) because it is a large and unique community. It is more than likely that the average high school student will mention the most well-known members of the IC such as the FBI, the CIA, and the NSA based on modern day television and movies. However, it is important to emphasize that the *who* is not nearly as important as the *what* because the IC must work diligently to collaborate and coordinate across agencies given the unique skillsets and missions of the respective organization.

There are 17 agencies in the Intelligence Community, within the majority of these agencies, a person entering the Intelligence field may have an analytical focus, an operational focus, or a technical focus. Introduction to the "intelligence careers" page (resource #1) will be a great introduction of where students can find more information on summer internship programs (for high school as well as college students). Resource #2 ("ODNI, Members of the IC") includes links to the homepage for each member organization. Note: *I recommend using the link below to facilitate a practical exercise in which groups of students are assigned between one and three organizations and answer questions such as: (1) What are the organizations' unique mission(s)? (2) Do employees of the respective organization focus on analysis, support operations, have more technical backgrounds or a combination of all of these?*

Resources:

1. Who is the IC: https://www.intelligencecareers.gov/icmembers.html
   - Includes 3 minute video: https://youtu.be/2b_NCvcniRc (the speakers in this video represent the importance of diversity in the IC)
2. ODNI: "Members of the IC" https://www.dni.gov/index.php/what-we-do/members-of-the-ic

SSIUSINS2 – Describe the basic roles and functions of the Intelligence field.

d. Explain the security clearance process (e.g., include barriers to acquiring the various types).

The application process for a career in the intelligence field may seem daunting because it is a time-consuming process. But the benefits are well worth the effort. There are five areas explained: (1) obtaining a security clearance, (2) citizenship, (3) drug use, (4) personal integrity and conduct, and (5) medical fitness. There is also a video that explains the polygraph to assuage concerns and address common myths – the polygraph is a requirement for the majority of agencies within the IC. Employees within the Intelligence Community require a high degree of integrity, discipline, and honor. Note*: It is worth explaining to students that some organizations (like the FBI) have a strict drug use policy – they will not consider applicants that have used drugs within the last 10 years.*

Resources:

1. Intelligence Careers "Application Process"
https://www.intelligencecareers.gov/icapply.html
2. Intelligence Careers "The Polygraph Exam"
https://www.youtube.com/watch?time_continue=46&v=YofC998l-qo&feature=emb_logo

SSIUSINS2 – Describe the basic roles and functions of the Intelligence field.

e. Describe levels of vulnerability for Intelligence Security.

Intelligence is only valuable when it is safeguarded. The nation's adversaries constantly try to find vulnerabilities to exploit and gain access to intelligence and subsequently change the dynamics of decision advantage. The process of protecting intelligence is called **counterintelligence**. Counterintelligence (CI) is defined by the National Security Act of 1947 and the goal of CI programs is to identify, disrupt, and protect against espionage and sabotage conducted on behalf of foreign entities. The **National Counterintelligence and Security Center** (NCSC) is a component of the Office of the Director of National Intelligence that is responsible for leading and supporting the U.S. government's counterintelligence and security activities. This organization also conducts outreach with U.S. private sector entities that are at risk of foreign intelligence penetration. The NCSC has several focus areas to include threat assessments, personnel security, insider threat, damage assessments, information sharing, physical security, supply chain risk management, and cyber threats.

Security threats posed by foreign intelligence entities is an important aspect to discuss with the students because the personnel working within the IC are constant targets of foreign intelligence services. Some common foreign collection methods include overt or covert solicitation of information (via social media, in academic institutions, at conferences, and while traveling abroad). See **ICD 750** for information on the Counterintelligence program. There is a common acronym describing how foreign intelligence services attempt to lure (often unsuspecting) IC

employees to betray their country. This acronym is **MICE** and it stands for: money, ideology, coercion (or compromise), and ego (or excitement). However, another (less common, but equally important) acronym is **RASCLS** and it stands for: reciprocation, authority, scarcity, commitment (or consistency), liking, and social proof. Some historic examples of Americans that became spies for other countries are discussed in SSIUSINS1c under "Year of the Spy." You could use either MICE or RASCLS when examining those case studies and determining *why* and *how* someone chose to betray their country.

Note: *I recommend showing the FBI video "Game of Pawns" that is based on true events. It demonstrates general ways humans can fall victim to providing sensitive information. You could use both MICE and RASCLS to examine the various components that may have influenced the main actor to provide sensitive information to a foreign country.*

Resources:

1. NCSC, "What we Do," https://www.dni.gov/index.php/ncsc-home
2. FBI, "Game of Pawns" https://www.youtube.com/watch?v=R8xlUNK4JHQ
3. ODNI, "Intelligence Community Directive 750: Counterintelligence Programs," https://www.dni.gov/files/documents/ICD/ICD750.pdf
4. Burkett, "From MICE to RASCLS" https://www.cia.gov/static/3e909813c3f24ffea6481524038bcace/Alt-Framework-Agent-Recruitment.pdf

SSIUSINS3 – Explore the different types of Intelligence, collection methods, and information sharing.

a. Identify the six basic intelligence sources and methods of collection and explain their uses (Signals Intelligence (SIGINT/aka COMINT), Measurement and Signature Intelligence (MASINT), Human Intelligence (HUMINT), Open-Source Intelligence (OSINT), Geospatial Intelligence (GEOINT/formerly IMINT)).

It is important to note that a discussion on each intelligence discipline could take a full day. The following excerpts and links are intended to provide enough information to provide an overview and assign a practical exercise to facilitate discovery and peer-to-peer learning. One central point for an overview of each intelligence discipline is the Director of National Intelligence website: https://www.dni.gov/index.php/what-we-do/what-is-intelligence. However, where applicable, there are additional links provided under each intelligence discipline.

Signals Intelligence (SIGINT): The National Security Agency is responsible for providing foreign Signals Intelligence (SIGINT) to our nation's policy-makers and military forces. SIGINT plays a vital role in our national security by providing America's leaders with critical information they need to defend our country, save lives, and advance U.S. goals and alliances globally. NSA's SIGINT mission is specifically limited to gathering information about international terrorists and foreign powers, organizations, or persons. NSA produces intelligence in response to formal requirements levied by those who have an official need for intelligence, including all departments of the Executive Branch of the United States Government.

Resource for SIGINT: https://www.nsa.gov/what-we-do/signals-intelligence/

Measurement and Signature Intelligence (MASINT): The Directorate for MASINT and Technical Collection (DT), a component of the Defense Intelligence Agency, is the focus for all national and Department of Defense MASINT matters. Measurement and Signature Intelligence is technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. Examples of this might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. MASINT is a science-intensive discipline that needs people/scientists well versed in the broad range of physical and electrical sciences.

Resource for MASINT: https://www.dni.gov/index.php/what-we-do/what-is-intelligence

Human Intelligence (HUMINT): Throughout history, information derived from human sources has helped shape foreign policy decisions. If Oleg Penkovsky had not been providing the CIA with detailed information regarding the Soviet's missile capabilities, the Cuban Missile Crisis might have had a completely different outcome. Human intelligence (HUMINT) is defined as any information that can be gathered from human sources. The National Clandestine Service (NCS) is the branch of the CIA responsible for the collection of HUMINT. The NCS is charged with strengthening national security and foreign policy objectives through the clandestine collection of HUMINT. HUMINT is collected through: clandestine acquisition of photography, documents, and other material; overt collection by people overseas; debriefing of foreign nationals and U.S. citizens who travel abroad; and official contacts with foreign governments. It is important to note that the CIA is not the only organization within the intelligence community that conducts HUMINT. For example, law enforcement agencies (e.g., the FBI and the DEA) use HUMINT and the various branches of military service as conduct HUMINT.

Resource for HUMINT: https://www.dni.gov/index.php/what-we-do/what-is-intelligence

Open-Source Intelligence (OSINT): The CIA is responsible for collecting, producing, and promoting open source intelligence through its management of the DNI Open Source Enterprise. Information does not have to be secret to be valuable. Whether in the blogs we browse, the broadcasts we watch, or the specialized journals we read, there is an endless supply of information that contributes to our understanding of the world. The Intelligence Community generally refers to this information as Open Source Intelligence (OSINT). OSINT plays an essential role in giving the national security community as a whole insight and context at a relatively low cost. OSINT is drawn from publicly available material, including: the internet; traditional mass media (e.g., television, radio, newspapers, magazines); specialized journals, conference proceedings, and think tank studies; photos; and geospatial information (e.g., maps and commercial imagery products).

Geospatial Intelligence (GEOINT): The National Geospatial-Intelligence Agency has a responsibility to provide the products and services that decision makers, military service members, and first responders need, when they need it most. As a member of the Intelligence Community and the Department of Defense, NGA supports a unique mission set. We are committed to

acquiring, developing and maintaining the proper technology, people and processes that will enable overall mission success. Geospatial intelligence, or GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, imagery intelligence and geospatial information.

Resource for GEOINT: https://www.nga.mil

- Includes a 3-minute video "Show the Way" https://youtu.be/VIKnYyszDYg

SSIUSINS3 – Explore the different types of Intelligence, collection methods, and information sharing.

b. Describe other sources and types of Intelligence such as: Medical Intelligence, Cyber Threat Intelligence, Environmental Intelligence, Economic and Competitive Intelligence, Law Enforcement Intelligence, Cultural Intelligence, Strategic Intelligence, and Financial Intelligence.

Medical Intelligence: The need for a professional medical intelligence capability was made abundantly clear during the Spanish influenza epidemic in the midst of the First World War. In the interwar years, the surgeon general established medical intelligence support by providing detailed guides for civil public health and sanitation conditions to help prevent a similar epidemic-like situation. As the likelihood of the U.S. entering into World War II increased, the need for an organized staff became a high priority. Fast forward to 1963, DIA absorbed medical intelligence as a division of its production branch. Although temporarily pulled from DIA's missions, Congress mandated the permanent transfer of the organization, then called the Armed Forces Medical Intelligence Center, to DIA in 1992. In July 2008, leaders from across the U.S. Intelligence Community dedicated the **National Center for Medical Intelligence (NCMI)** at a ribbon cutting ceremony at Ft. Detrick, Maryland. The NCMI is the critical link between Department of Defense force protection and broader homeland health protection. It demonstrates the vital contribution that medical intelligence makes to public health security.

Resource: DIA https://www.dia.mil/News/Articles/Article-View/Article/1902266/this-week-in-dia-history-national-center-for-medical-intelligence-hits-double-d/

Cyber Threat Intelligence: Cyber threat intelligence is the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, and their impact or potential effects on U.S. national security interests. Cyber threat intelligence also includes information on cyber threat actor information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign cyber program information systems. The **Cyber Threat Intelligence Integration Center (CTIIC)** is the federal lead for intelligence support in response to significant cyber incidents, working on behalf of the IC to integrate analysis of threat trends and events, build situational awareness, and support interagency efforts to develop options for degrading or mitigating adversary threat capabilities. CTIIC is an integration point where analysts scrutinize fragments of cyber threat information produced by network defenders,

Intelligence Community, law enforcement, incident responders, and non-Government sources; make connections; place the activity in context; call attention to significant activity; and work with partners to develop whole-of-government approaches to mitigate or counter the threat.

Resources:

1. ODNI, "2019 National Intelligence Strategy" https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
2. CTIIC, "Who we Are," https://www.dni.gov/index.php/ctiic-who-we-are

Environmental Intelligence: The term **environmental intelligence** is not as common as the other types of intelligence. However, understanding the weather and the environment is an important part of intelligence analysis. For example, when planning military operations, weather considerations is a key factor in planning the date, time, and location of activity. Moreover, the impacts of climate change are another important consideration. Climate change is projected to produce more intense and frequent extreme weather events, multiple weather disturbances, along with broader climatological effects, such as sea level rise. These are almost certain to have significant direct and indirect social, economic, political, and security implications during the next 20 years. These effects will be especially pronounced as populations continue to concentrate in climate-vulnerable locales such as coastal areas, water- stressed regions, and ever-growing cities. These effects are likely to pose significant national security challenges for the United States over the next two decades, though models forecast the most dramatic effects further into the future. While specific extreme weather events remain difficult to attribute entirely to climate change, unusual patterns of extreme and record-breaking weather events are likely to become more common, according to the Intergovernmental Panel on Climate Change (IPCC).

The **National Oceanic and Atmospheric Administration** (NOAA) is America's environmental intelligence agency. From daily weather forecasts, severe storm warnings and climate monitoring to fisheries management, coastal restoration and supporting marine commerce, NOAA's products and services enrich life through science and support economic vitality. NOAA's dedicated scientists use cutting-edge research and high-tech instrumentation to provide citizens, planners, emergency managers and other decision makers with reliable information they need when they need it.

Resources:

1. NOAA, "Our history" https://www.noaa.gov/our-history
2. DNI "Implications for US National Security of Anticipated Climate Change," https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Implications_for_US_National_Security_of_Anticipated_Climate_Change.pdf

Economic and Competitive Intelligence: This term is not commonly used within the intelligence community. When intelligence is gathered by public services it is referred to as "economic intelligence," but when the intelligence is gathered by companies, it is called "competitive intelligence." However, this term is associated with counterintelligence efforts. Specifically, the National Counterintelligence and Security Center (which is part of the ODNI) published the *National Counterintelligence Strategy of the United States of America 2020-2022*. This strategy outlines key components of economic and competitive intelligence as it pertains to

national security considerations. As noted in the strategy, foreign intelligence actors—to include nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure, and steal sensitive information, research, technology, and industrial secrets. Many countries target the United States because it is a global center for high-technology research, technology and innovation. Foreign intelligence entities have embedded themselves into U.S. national labs, academic institutions, and industries that form America's national innovation base. They have done this to acquire information and technology that is critical to the growth and vitality of the U.S. economy. Adversaries use front companies, joint ventures, mergers and acquisitions, foreign direct investment, and talent recruitment programs to gain access to and exploit U.S. technology and intellectual property. They also influence and exploit U.S. economic and fiscal policies and trade relationships.

Resource: NCSC "National Counterintelligence Strategy 2020-2022"
https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf

Law Enforcement Intelligence: The FBI, as an intelligence and law enforcement agency, is responsible for understanding threats to our national security and penetrating national and transnational networks that have a desire and capability to harm the U.S. The Intelligence Branch is the strategic leader of the FBI's Intelligence Program and drives collaboration to achieve the full integration of intelligence and operations, and it proactively engages with the Bureau's partners across the intelligence and law enforcement communities. By overseeing intelligence policy and guidance, the Intelligence Branch ensures the FBI's intelligence production remains objective and strikes the correct balance between strategic and tactical work.

The FBI has always used intelligence to investigate and solve cases. Throughout the Bureau's history, its ability to successfully adapt to new threats included the development of increasingly sophisticated methods of gathering, analyzing, and disseminating intelligence. The FBI history page provides a glimpse of the Bureau's intelligence role from its founding to the present day. In the aftermath of the 9/11 terrorist attacks, the FBI recognized the need to establish centralized control over intelligence operations throughout the Bureau. The FBI was first directed to create a Directorate of Intelligence through a November 23, 2004 presidential memorandum for the attorney general (titled "Further Strengthening Federal Bureau of Investigation Capabilities") and later through The Consolidated Appropriations Act of 2005. The Intelligence Reform and Terrorism Prevention Act of 2004 reiterated this guidance and formally acknowledged the significant progress made by the FBI in improving its intelligence capabilities since the 9/11 attacks.

The Directorate of Intelligence was established in February 2005 as a dedicated national intelligence workforce within the FBI—a service within a service. The central mission of the FBI's Intelligence Program is to optimally position the Bureau to meet current and emerging national security and criminal threats. The Bureau does this in cooperation with its partner intelligence organizations. Citing the continued evolution of the FBI's Intelligence Program, the Intelligence Branch was created in August 2014. The Directorate of Intelligence, Bureau

Intelligence Council, and Office of Partner Engagement are now part of the branch, under the leadership of an Executive Assistant Director.

Resource: FBI, "Intelligence Branch" https://www.fbi.gov/about/leadership-and-structure/intelligence-branch

Cultural Intelligence: Unlike the other intelligence disciplines and/or focus areas in this section, cultural intelligence is often used to describe the development of cultural knowledge. One need only review U.S. geopolitical failures (e.g., the Vietnam War, the Iranian Revolution, and the wars in Iraq and Afghanistan) to observe the lack of cultural knowledge that in many examples impacted the success (or lack thereof) of the U.S. achieving its strategic objectives.

Resource: CIA, "Cultural Intelligence"
https://www.cia.gov/static/c65ef854238e04ac8a7a6d9c5119559d/Individual-Interactions-Across-Cultures.pdf

Strategic Intelligence: When analysts are studying long-term issues and providing intelligence products for senior leaders and policy makers it is consider strategic intelligence. As defined in the 2019 National Intelligence Strategy, it is the process and product of developing the context, knowledge, and understanding of the strategic environment required to support U.S. national security policy and planning decisions. This work includes identifying and assessing the capabilities, activities, and intentions of states and non-state entities to identify risks to and opportunities for U.S. national security interests. Strategic intelligence involves assimilating a variety of information—including knowledge of political, diplomatic, economic, and security developments—to create a deep understanding of issues of enduring importance to the United States. Strategic intelligence also provides in-depth assessments of trends and developments to recognize and warn of changes related to these issues that will affect the future strategic environment. The foundation for strategic intelligence requires developing and maintaining a deep understanding of the strategic environment, to include transnational issues such as terrorism and transnational organized crime, and the capabilities, activities, and intentions of states and non-state entities necessary to support U.S. national security policy and planning decisions.

Resource: ODNI, "2019 National Intelligence Strategy" (page 8).
https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

Financial Intelligence: Economic funding is critical in any operation conducted by adversaries. The Department of Treasury plays a significant role in the collection and analysis of financial transactions ("the money trail").

As noted by the Department of Treasury, intelligence has played an important role in the exercise of the responsibilities and operations of the Department since the assumption of its enforcement responsibilities in 1789. The **Office of Terrorism and Financial Intelligence (TFI)** marshals the department's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats.

Two components of TFI are led by Assistant Secretaries. The Office of Terrorist Financing and Financial Crimes (TFFC), is the policy and outreach apparatus for TFI. The Office of Intelligence and Analysis (OIA) is responsible for TFI's intelligence functions, integrating the Treasury Department into the larger intelligence community (IC), and providing support to both Treasury leadership and the IC.

TFI also oversees several component offices and bureaus. The Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions. The Treasury Executive Office for Asset Forfeiture (TEOAF) administers the Treasury Forfeiture Fund (TFF), which is the receipt account for the deposit of non-tax forfeitures. Responsible for administering the Bank Secrecy Act (BSA) and other regulatory functions is one of Treasury's bureaus, the Financial Crimes Enforcement Network (FinCEN), which supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns. The director of FinCEN reports directly to the Under Secretary. TFI also works in close partnership with the IRS Criminal Investigative Division (IRS-CI) to enforce laws against terrorist financing and money laundering, including the Bank Secrecy Act.

Resource: U.S. Department of Treasury, "Terrorism and Financial Intelligence," https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence

SSIUSINS3 – Explore the different types of Intelligence, collection methods, and information sharing.

c. Compare and contrast the strengths and weaknesses inherent in the various sources and types of Intelligence in SSIUSINS3a-b.

It is imperative to demonstrate that within the intelligence community exists the consistent need to examine intelligence from all available sources. This form of analysis is called all-source intelligence analysis. As the name suggests, the best way to provide the best situational awareness to policy and decision makers is for intelligence professionals (regardless of their organizations) to examine all forms of intelligence because each type of intelligence has inherent weaknesses. For example, GEOINT requires mostly expensive equipment that can be impacted by weather conditions. It may also take GEOINT analysts time to process and exploit the image to provide analysis. Another example is HUMINT where the intelligence is derived from a human. The challenge here is access (to people with information) and validation (ensuring the information provided is accurate and free of deception). Note: *It may be helpful to give the students a benign scenario where they need to find information about an event. Ask them to identify if/how each intelligence discipline could be utilized. That exercise will help with comparing and contrasting strengths and weaknesses of various sources of information.*

SSIUSINS3 – Explore the different types of Intelligence, collection methods, and information sharing.

d. Explore current trends in different types of Intelligence that challenge collection methods.

The scrutiny of intelligence collection increased following 9/11 (via the 9/11 Commission Report and subsequent Intelligence Reform and Terrorism Prevent Act of 2004), then again after the release of classified information by Chelsea Manning (in 2009-2010) and Edward Snowden (in 2013). In addition to this scrutiny, the increased use of technology has also created challenges in intelligence collection. Another consideration is how the digital age is redefining intelligence operations and collections. Some examples include, nation-state competition in space, cyberspace capabilities, the use of artificial intelligence and machine learning, and the increased use of denial and deception to influence people (such as fake news, fake images, and erroneous information distributed across the internet). Note: *This is a rather fluid topic, I recommend reviewing resources such as RAND (see link below) to gain perspective on the current and projected challenges.*

Resource: RAND, "Intelligence Collection" https://www.rand.org/topics/intelligence-collection.html

SSIUSINS3 – Explore the different types of Intelligence, collection methods, and information sharing.

e. Explain how recent events affect how information is shared with partner nations.

When classified information is leaked, that information could negatively impact relationships with foreign partner nations. However, the partnerships have remained intact because they remain a vital component of combating adversaries whose actions have global impacts such as terrorism and cyberspace operations. The counterterrorism mission and efforts to secure critical infrastructure are great examples.

The counterterrorism mission requires sharing many types of terrorism-related information, for example, the exchange of biographic and biometric information related to known or suspected terrorists. While such sharing often includes classified information and sensitive diplomatic, law enforcement, and homeland security information relating to terrorism, it also encompasses other information that, over time, may help reveal links to terrorist groups or individuals. Information regarding lost or stolen passports and suspect financial transactions, for example, might yield information on groups or persons who subsequently are linked to a specific terrorist threat. In addition to asking for such information from other countries, the U.S. strives to appropriately share similar types of information with foreign governments or foreign law enforcement entities, such as INTERPOL, as long as the sharing of any records about American citizens and lawful permanent residents' data is subject to the *Privacy Act of 1974* limitations, especially regarding personally identifiable information.

Information sharing with foreign partners is a key component of international outreach and cooperation to protect U.S. critical infrastructure. Given the often sensitive nature of the information shared, the U.S. may enter into agreements and other understandings with foreign governments to ensure appropriate security and confidentiality of exchanged information.

Resource: "National Strategy for Information Sharing" https://www.hsdl.org/?view&did=480495

SSIUSINS4 – Analyze the Intelligence Cycle.

a. Describe the stages of the Intelligence Cycle (e.g., Planning, Collection, Processing & Exploitation, Analysis & Production).

There are multiple versions of the intelligence cycle. However, the graphics depicted in this section can be found in two government documents and demonstrate the interconnectivity of the stages within the cycle. It is important to acknowledge that this six-step process is cyclical and never-ending because the profession of intelligence analysis is a continuous process – our adversaries continue to plan and conduct operations, therefore intelligence analysis and operations are continuous. The stages of the intelligence cycle are: (1) planning and direction, (2) collection, (3) processing and exploitation, (4) analysis and production, (5) dissemination, and (6) feedback and evaluation.

Planning and direction: Intelligence operations and analysis will always be connected to a mission. Oftentimes the intelligence consumer (often the policy or decision maker, and sometimes agencies within the intelligence community) will identify an intelligence requirement. The consumer may request a product that can be a report, a graphic image, an oral presentation, or raw information. Based on the requirement, the intelligence organization that receives the task will begin planning intelligence activities to fulfill the consumer's request.

Collection: During the collection phase intelligence professionals are gathering raw (unprocessed) data that is required to produce a finished intelligence product. There are five basic intelligence sources (discussed in **SSIUSINS3a**) where data collection is performed: GEOINT, HUMINT, MASINT, OSINT, and SIGINT. Some examples of raw data include news reports, aerial imagery, satellite imagery, government and public documents, or word of mouth.

Processing and Exploitation: The conversion of raw data into a comprehensible format that can be used in a finished intelligence product is a very important stage of the intelligence cycle. Oftentimes, this stage involves specialist and technical equipment. It can also involve data decryption, data translation, and the interpretation of imagery.

Analysis and Production: During this stage, processed information is integrated, evaluated, and analyzed to develop a deeper understanding of the environment. Essentially, the synthesis of processed information is required to explain the "so what." If the consumer only wants the raw data, then this stage may be skipped. However, if the consumer wants an all-source intelligence product, then this stage becomes significant.

Dissemination: During this stage, the processed information is disseminated to the consumer in whatever form requested (e.g., electronic transmission, a printed document, or an oral

presentation). While it may seem natural to be "finished" once the product is disseminated, this is not the case. It is common for the dissemination of a product to generate additional questions – and if so, the intelligence cycle begins all over again.

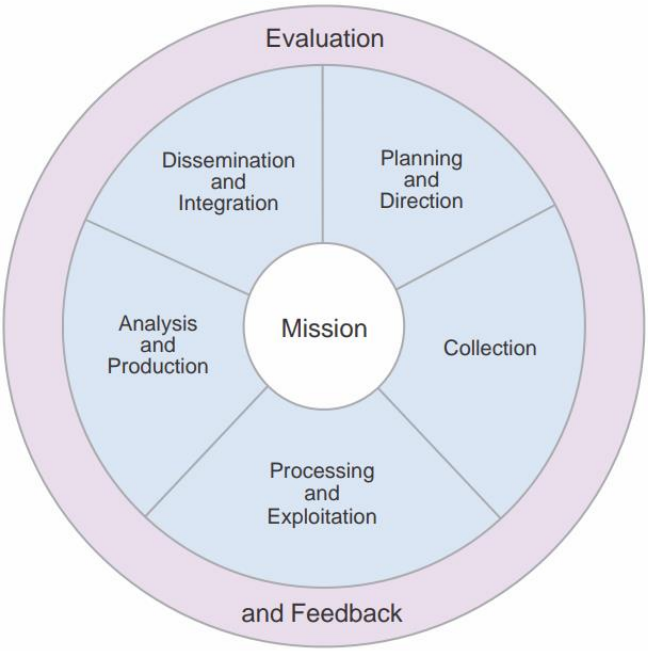
Evaluation and Feedback: Sometimes this stage is overlooked, but it too is significant. The consumer should provide feedback to the intelligence collectors, operators, and analysts so all of the intelligence professionals involved can refine their collection methods or analysis as required. For the aforementioned intelligence disciplines, feedback is very important to continued collection of information.

> Example: a notional consumer requests an all-source intelligence analysis to answer the question of whether or not a facility in a particular country is involved in nefarious nuclear activity. The intelligence in support of this request include images of the facility, MASINT analysis of water near that facility, and a HUMINT report from someone that works inside the facility. The consumer should evaluate the intelligence received and explain how the data were helpful. This could provide the following feedback: 1) It confirms that the imagery collection process is correct in the direction and timing for collecting images of that facility; 2) It confirms the MASINT collection was beneficial (so the process, the location, and the analysis was correct); 3) It confirms, in this particular case, whether or not the information provided by the person working in the facility was accurate.

The Six Steps in the Intelligence Cycle

The Intelligence Cycle is the process of developing raw information into finished intelligence for use by policymakers, military commanders, and other consumers in decision making. This six-step cyclical process is highly dynamic, continuous, and never-ending. The sixth step, evaluation (which includes soliciting feedback from users) is conducted for each of the other five steps individually and for the Intelligence Cycle as a whole.

Graphic: Intelligence cycle from ODNI overview.



Graphic: Intelligence cyber from JP 2-0

Resources:

1. ODNI, An Overview on the Intelligence Community (2013): https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf
2. Joint Chiefs of Staff, Joint Intelligence (JP 2-0): https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

SSIUSINS4 – Analyze the Intelligence Cycle.

b. Distinguish between raw and finished intelligence.

Inherent in the discussion about intelligence is the important distinction between information and intelligence. All information is not intelligence because information is unprocessed material, but intelligence is derived from information. A further discussion between raw and finished intelligence has been covered in SSIUSINS4a regarding the stages of the intelligence cycle. But a simple example is the application of OSINT. Anyone can read or listen to a news report (raw data and just basic information). However, as discussed in SSIUSINS3a, OSINT is the process of analyzing that publicly available material for authenticity and deeper meaning. For example, it can provide insight to how a particular foreign entity reacts to a speech by the U.S. president or other geopolitical activity. Rather than relying on an "official" statement by an organization or a nation-state, OSINT enables intelligence analysts to analyze authentic resources to get a better understanding of the environment.

SSIUSINS4 – Analyze the Intelligence Cycle.

c. Explain how to be successful at each stage of the Intelligence Cycle and describe the strengths and weaknesses of the current model.

Part of the successful application of the intelligence cycle involves respecting the process of each stage. If a baker were making a cake, he/she would ensure the oven was at the correct temperature; that all of the ingredients were added and mixed properly; and that the mixture was placed in the appropriate pan based on the desired end-state (e.g., a bundt cake, a multi-layered cake, or a cake that will become part of a larger design). In that same vein, intelligence professionals should adhere to all stages of the cycle where possible. The desired product may dictate whether all stages of the intelligence cycle are necessary (e.g., the consumer may simply want a raw image of a facility). As noted in **SSIUSINS4a,** there is not one agreed upon model for the intelligence cycle and perhaps that is where the greatest weakness lies. Nevertheless, explaining the cycle using one or both of the models in SSIUSINS4a will demonstrate the importance of the intelligence process as well as the coordination and collaboration required of intelligence collectors, operators, and analysts to develop the complete picture of the environment.

SSIUSINS5 – Evaluate the role of an Intelligence Analyst.

a. Describe the role of an analyst in assessing the value of information.

The analyst's role of assessing the value of information is a mixture between understanding the operational environment and knowing the benefits of using multiple sources of intelligence. The Intelligence Community Directive (ICD) 203 underscores the responsibility of analysts to strive for excellence, integrity, and rigor when conducting intelligence analysis. Specifically, analysts should strive to ensure they objectively assess the environment based on all available sources of intelligence information and be forthcoming about information they do not know because of information gaps or because of information that may not be deemed credible (like a walk-in HUMINT source that wants a lot of money for information that cannot be completely verified) or that may not be high quality (like an image that has poor resolution or extreme cloud cover). Essentially, when an analyst assesses the value of information it should be done in a manner that is objective. Note: *This is likely a topic best paired with SSIUSINS5 below. ICD 203 and the structured analytic techniques are intended to improve the analysts' overall ability to assess both the information and the environment by using techniques that limit bias and encourage intellectual humility (the ability to clearly state what one does not know) among other intellectual traits.*

Resources:

1. ODNI, "Analytic Standards" https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

SSIUSINS5 – Evaluate the role of an Intelligence Analyst.

b. Explain how analysts use structured analytic techniques such as analysis of competing hypotheses and key assumptions check.

Quote: *Analysts must absorb information with the thoroughness of historians, organize it with the skill of librarians, and disseminate it with the zeal of journalists.* - General Michael T. Flynn

This quote is a personal favorite because it demonstrates (1) the expectation of intelligence analysts by senior decision makers and (2) the complexity of intelligence analysis. The implementation of analytic standards and analytic tradecraft standards (as discussed in ICD 203) is paramount to producing intelligence that meets the required rigor and integrity. There are a series of structured analytic techniques (SATs) that serve as tools to challenge mindset challenges and cognitive biases, identify potential solutions to complex problem sets, and enables analysts to demonstrate *how* they make sound judgments and reach unbiased and unpoliticized conclusions. There are techniques such as various forms of brainstorming like mind maps and starbursts. There are also a variety of diagnostic techniques such as checking one's assumptions (Key Assumptions Check), identifying indicators or signposts of change, and considering multiple plausible hypotheses to address a key question (Analysis of Competing Hypotheses). Note: *Explaining how analysts use SATs could easily become a multi-day process. However, please see the free resources below that explain the challenges of cognitive biases (resource #1) and examples of how to apply different types of SATs (resource #2).*

Resources:

1. CIA, "Psychology of Intelligence Analysis," https://www.cia.gov/resources/csi/books-monographs/psychology-of-intelligence-analysis-2/
2. CIA, "A Tradecraft Primer: SATs for Improving Intelligence Analysis," https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf

SSIUSINS5 – Evaluate the role of an Intelligence Analyst.

c. Describe the authorized activities (military/civilian, international/domestic) of each of the federal agencies comprising the Intelligence Community.

Given the history of intelligence, covered in SSIUSINS1a.-d., one can respect the need (over the years) for better oversight. The various authorizations of each of the federal agencies can be further research at the ODNI page under "Oversight & Partners."

SSIUSINS5 – Evaluate the role of an Intelligence Analyst.

d. Explain the purposes and processes for sharing of information between U.S. Intelligence agencies.

One of the revelations from the 9/11 Commission Report was the abysmal rate of information sharing between agencies before the September 11, 2001 terrorist attacks. I am not suggesting

students be given the 9/11 Commission Report to read, however, it may be worth reiterating the reforms within the intelligence community as a result of the September 11, 2001 terrorist attacks, especially the Intelligence Reform and Terrorism Prevention Act of 2004.

At the organizational level, ODNI has established the Information Sharing Environment. The Information Sharing Environment (ISE) consists of the people, projects, systems, and agencies that enable responsible information sharing across the national security enterprise. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004 and a direct result of 9/11 Commission recommendations. Law enforcement, defense, and intelligence personnel rely on timely and accurate information to keep America safe, and the ISE makes that happen by:

- Advancing responsible information sharing to further counterterrorism, homeland security, and counter weapons of mass destruction missions
- Improving nationwide decision making by transforming from information ownership to stewardship
- Promoting partnerships across federal, state, local, and tribal governments, the private sector, and internationally

In the case of sharing information, between U.S. intelligence agencies at the individual analyst level, analysts should strive to ask themselves "who else (with the appropriate clearance) needs to know this information?" Ultimately, the process of sharing information involves the establishment and maintenance of relationships between people and partnerships between organizations. It is a continuous process.

Resource: ODNI, "About the ISE," https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise

SSIUSINS5 – Evaluate the role of an Intelligence Analyst.

e. Describe the role of Fusion Centers in coordinating federal and state information sharing.

As the name suggests, fusion centers are intended to be a central point for gathering, analyzing, and sharing information across organizations and agencies at various levels of government. In a post-9/11 world communication, coordination, and collaboration are critical components of effective all-source analysis. Prior to 9/11, the information flow between federal, state, local, tribal, and territorial partners was not sufficiently robust to achieve a strong, effective, and productive nationwide information sharing partnership. Today, fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial and private sector partners. To support these information sharing efforts, federal agencies have improved coordinating the planning and provision of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding, in support of the National Network of Fusion Centers.

Fusion centers contribute to the Information Sharing Environment (ISE) through their role in receiving threat information from the federal government; analyzing that information in the

context of their local environment; disseminating that information to local agencies; and gathering tips, leads, and suspicious activity reporting (SAR) from local agencies and the public.

Resource: ODNI, "National Network Fusion Centers," https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/ise-archive/ise-additional-resources/2119-national-network-of-fusion-centers?highlight=WyJmdXNpb24iLCJjZW50ZXJzIiwiY2VudGVyIiwiY2VudGVyJ3MiLCInY2VudGVyIiwiY2VudGVyZWQiLCInY2VudGVycyIsImNlbnRlcnMnIiwiY2VudGVyaW5nIiwiZnVzaW9uIGNlbnRlcnMiXQ==

SSIUSINS6 – Analyze the ethical, moral, and legal considerations of Intelligence.

a. Describe how ethical standards and moral dilemmas challenge intelligence analysts as they relate to secrecy, war and peace, ends versus means, nature of the opponent, and national interest.

The ODNI has published the principles of professional ethics for the intelligence community that reflect the core values and standards common to all elements of the IC.

Regarding covert action, the possibility of collateral damage and blowback has historically been something the U.S. has endured. An example of this would be the U.S. arming and training of Afghan fighters during the Soviet War in Afghanistan. Another example is U.S. support to anti-Assad factions in Syria. The challenge remains knowing the long-term impacts of involvement. In the case of Afghanistan, the U.S. ceased support to the nation once the Soviet Union fell and left a political vacuum in the country. Some scholars believe that vacuum set the conditions for what would become a greater threat to the U.S. over 20 years later.

There have been two recent examples of intelligence analysts that released classified information due to a reported moral and ethical dilemma (Chelsea Manning and Edward Snowden). However, it is important to note there are structures in place to enable an intelligence professional to follow a procedure to voice their concerns without releasing classified information that can have catastrophic impacts to intelligence professionals across the globe. Intelligence professionals should never do anything that is illegal, immoral, or unethical. The Presidential Policy Directive-19 (PPD-19) provides protections for IC employees that participate in the whistleblowing process. Furthermore, every organization within the IC has a process for employees that make a lawful disclosure of questionable activity.

Resources:

1. Washington Institute, "Who is responsible for the Taliban," https://www.washingtoninstitute.org/policy-analysis/view/who-is-responsible-for-the-taliban
2. ODNI, "Making Lawful Disclosures," https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-related-menus/icig-related-links/making-lawful-disclosures

SSIUSINS6 – Analyze the ethical, moral, and legal considerations of Intelligence.

b. Explain how changes over time in societal ethics and morality, both domestic and foreign, affect intelligence officers.

The notion of collecting information, convincing a person to betray their country or loved ones, and manipulating individuals to cooperate can create ethical and moral dilemmas among intelligence analysts, operators, and collectors. Furthermore, the process of working as a targeting analysts (some that provides intelligence and information to hunt and capture individuals) can also create moral dilemmas.

Another challenge for intelligence professionals is the possibility of politicizing intelligence. The politicization of intelligence could occur from the top-down (a supervisor dictating the production of intelligence to achieve a political agenda) or from the bottom-up (intelligence analysts independently altering information to appease their supervisor or policy/decision maker). Intelligence professionals have the responsibility to provide policy makers and decision makers with information that they *need* to hear, which is not always what they may *want* to hear.

Resource:

1. Robert Gate's "Guarding Against Politicization," https://www.cia.gov/static/e6476fde888eb019dab6e45fc029f562/Guarding-Against-Politicization.pdf
2. The Harvard Gazette, Intelligence Project Conference, https://news.harvard.edu/gazette/story/2019/05/former-intelligence-officials-discuss-the-state-of-affairs-at-harvard/

SSIUSINS6 – Analyze the ethical, moral, and legal considerations of Intelligence.

c. Explain how Intelligence professionals relate ethical and moral issues to collection and covert action.

The practice of intelligence collection changes with the environment based on placement, access, resources, and technology. Likewise, the types of threats continue to change and require a consistent review of who may have the most valuable information. In many cases, bad guys have good information. Collaborating with people with questionable morals and ethics is often part of the information collection process. A fictional example of this is the Amazon series *Jack Ryan* in which a finance analyst working for the CIA finds himself in the field with an intelligence collector. Jack (the main character) finds himself in an ethical and moral dilemma when he has to collaborate with a known human trafficker (named Tony) to find someone that is a key part to his investigation. He finds himself disgusted by Tony and his obvious contempt is threatening the likelihood of Tony assisting his efforts. Note: *This show is rated R for violence and content.*

Another dilemma involves methods for retrieving information of value from detainees. Previous reports of abuse at detention centers such as Guantanamo Bay and Abu Ghraib have created a

use case of how information should not be obtained from a nation such as the United States that operate with a higher level of ethics and morals than other countries. In other words, the use of torture for intelligence collection purposes have been a catalyst to making explicit statements regarding what is acceptable behavior from U.S. intelligence collectors.

Resource: Bellaby, "What's the Harm? The Ethics of Intelligence Collection," https://www.researchgate.net/publication/254242801_What%27s_the_Harm_The_Ethics_of_Intelligence_Collection

SSIUSINS6 – Analyze the ethical, moral, and legal considerations of Intelligence.

d. Describe the legal constraints and challenges to the collection of intelligence domestically and abroad.

For the purpose of this course, students should know that intelligence professionals do not conduct collection without directives that include provisions based on legal authorities. Despite any television show or movie depicting intelligence operations, employees within the Intelligence Community do not operate without a mission, without legal authorities, and without guidance. The details regarding the various legal authorities can be found in the resource below.

Resource: ODNI, "Intelligence Community Legal Reference Book," https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf

SSIUSINS7 – Compare and contrast the roles and missions of the U.S. federal agencies comprising the U.S. Intelligence Community.

a. Identify all U.S. federal agencies which make up the U.S. Intelligence Community, including their functions and area of focus.

The U.S. Intelligence Community is composed of the following 17 organizations. A review of the links in the resources will describe their functions and area of focus:

- *Two independent agencies*—the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA).
- *Eight Department of Defense elements*—the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial- Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the four DoD services; the Army, Navy, Marine Corps, and Air Force.
- *Seven elements of other departments and agencies*—the Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Agency's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis.

Resources:

1. ODNI: "Members of the IC" https://www.dni.gov/index.php/what-we-do/members-of-the-ic *Note*: this website provides a link for each organization for comparison.
2. Intelligence Careers "Member Agencies" https://www.intelligencecareers.gov/icmembers.html Note: Graphics of each agency symbol available.

SSIUSINS7 – Compare and contrast the roles and missions of the U.S. federal agencies comprising the U.S. Intelligence Community.

b. Describe the role of the Director of National Intelligence in coordinating information sharing between agencies.

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Office of the Director of National Intelligence (ODNI), which began operating in 2005. By statute, the DNI is the principal intelligence adviser to the President and determines and manages the National Intelligence Program (NIP) budget of more than $50 billion, the U.S. government's total intelligence spending aside from military intelligence. The DNI is also tasked with integrating the efforts of the 17 elements of the IC.

The core mission of the ODNI is to lead the IC in intelligence integration, forging a community that delivers the most insightful intelligence possible. That means effectively operating as one team: synchronizing collection, analysis and counterintelligence so that they are fused. This integration is the key to ensuring national policymakers receive timely and accurate analysis from the IC to make educated decisions.

SSIUSINS7 – Compare and contrast the roles and missions of the U.S. federal agencies comprising the U.S. Intelligence Community.

c. Explain the role of Congress as an oversight body to the U.S. Intelligence Community.

The IC's authority to conduct intelligence activities is governed by numerous laws and regulations. Of primary importance is Executive Order 12333, United States Intelligence Activities. Most recently amended in 2008, the executive order sets strategic goals and defines roles and responsibilities within the IC, while also affirming the Nation's commitment to protect Americans' civil liberties and privacy rights in the conduct of intelligence activities.

Executive Order 12333 establishes this balance by prescribing general principles governing intelligence collection, retention and dissemination, and by specifying that intelligence activities concerning U.S. persons may only be conducted in accordance with procedures established by the element or department head and approved by the Attorney General, after consultation with the Director of National Intelligence.

Intelligence oversight is a mechanism to ensure that the IC conducts intelligence activities in a manner that that achieves the proper balance between the acquisition of essential information and protection of individual interests. The oversight is performed by entities inside and outside of the IC, which allows the IC to account for the lawfulness of its intelligence activities to the American

people, to Congress, to the President and to itself. ODNI engages and coordinates with the following entities in advance of actions where appropriate and provides reports or briefings of intelligence activities to the entities: the Intelligence Community, the Executive Branch, the Intelligence Oversight Board, the Privacy & Civil Liberties Oversight Board, the Office of Management and Budget, the Legislative Branch, and the Judicial Branch.

Resource: ODNI "Accountability" https://www.dni.gov/index.php/how-we-work/accountability