**KCA BISF CAT 1and 2 FOR Infrastructure in National security and intelligence (30 Marks)**

1. **Elaborate the critical activities that bring efficiency and effectiveness in intelligence (6 Marks)**

* Planning- is the process of figuring out what intelligence we need, how we are going to get it, and how we are going to make sure we get it. It is an essential part of the intelligence process, and it helps to ensure that the intelligence we produce is accurate, timely, and relevant.
* Collection- is the process of getting the intelligence information that is needed. This includes making sure that the right information is collected, that it is collected in a way that is efficient and effective, and that it is shared with the people who need it.
* Information sharing and collaboration- **When intelligence agencies share information and work together, they can do their jobs better. They don't waste time doing the same thing twice, and they have a better overall picture of what's going on.**
* Processing- is the process of making intelligence information more useful for analysts. This may involve making it easier to read, understand, or compare to other information.
* Investing in training and skill development-By providing intelligence personnel with the training and skills they need, intelligence agencies can improve their ability to gather, analyze, and disseminate intelligence, which can help them to better protect their countries and citizens from threats.

1. **Expound on the key design issues when integrating security measures (6 Marks)**

* Threat Modelling- threat modelling is a way to identify and understand the security risks posed to a system, so that you can design and implement appropriate security measures to mitigate those risks.
* Authentication and Authorization- authentication and authorization are used to ensure that only authorized users can access sensitive information and resources. Robust authentication and authorization mechanism is important to prevent unauthorized access to sensitive information.
* Secure Communication- **Secure communication is important to protect data from being seen or changed by unauthorized people.** This can be done by encrypting data, using secure APIs, and checking that user input is valid.
* Data Protection- It is keeping your information safe. This means using encryption to make your information unreadable to anyone who does not have the key to open them. You should also control who has access to your secrets and make sure that they are stored separately from other information.
* Secure Configuration-The process of setting up your systems and software in a way that makes them less vulnerable to attack.

1. **Explain some of the trends and technologies that have been adopted in security systems (6 Marks)**

* Internet of Things- IoT devices are any devices that can connect to the internet, such as smart TVs, thermostats, and doorbells. By implementing IoT security technologies, organizations can help to protect their smart devices and the data they collect from cyberattacks.
* Machine Learning and Artificial Learning- AI and ML algorithms can analyze massive datasets of security data, identify patterns and anomalies, and make predictions about potential threats in real time. This enables cybersecurity experts to detect and respond to threats more quickly and accurately than ever before.
* Blockchain Technology- is a distributed database that is secured by cryptography. It is most widely known for its role in powering cryptocurrencies, such as Bitcoin and Ethereum. However, blockchain has the potential to revolutionize cybersecurity as well. Blockchain technology has the potential to transform cybersecurity by providing a secure and tamper-proof way to store and share sensitive data.

**4. Is ethics is important when undertaking intelligence? If Yes, Explain why and if No Explain the reason (6 Marks)**

**5. Discuss some of the reasons why threats intelligence is important to organizations (6 Marks)**