**Prompt for Team and Cybersecurity Captain:**

**Context:** As the Cybersecurity Captain, your role is to guide your team in identifying, assessing, and mitigating potential cybersecurity risks associated with your AI solution that you believe will change the way public sector will address its problem. You will take on the role of Chief Information Security Officer (CISO) of this new company that provides this service/solution to public sector customers. Alternatively, you are the CISO of the public sector organization that will be directly implementing this solution on behalf of your citizens. Your goal is to collaborate with your teammates, conduct research, consult mentors, and leverage your own expertise to address the questions below. The goal is not to have perfect answers by the end of the hackathon, but rather to thoughtfully consider these critical cybersecurity aspects and refine your responses throughout the event. Your team will present your cybersecurity considerations along with your AI solution, and judges will evaluate your comprehensive approach. Best of luck!

**Threat Modeling and Risk Assessment:**

**Top-level question:** What are the key cybersecurity threats and risks associated with your AI solution, and how do you plan to mitigate them?

**Extra credit questions:**

Have you conducted a thorough threat modeling exercise to identify potential vulnerabilities and attack vectors?

How have you prioritized the identified risks based on likelihood and impact, and what specific measures have you implemented to address the most critical risks?

What processes do you have in place to continuously assess and update your risk model as new threats emerge or your AI solution evolves?

If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Asset Management and Data Security:**

**Top-level question:** How will you ensure the security and privacy of data used to train and operate your AI solution?

**Extra credit questions:**

Have you created an inventory of all AI assets, including models, data, and infrastructure components?

What data governance policies and practices have you established to ensure responsible data collection, storage, and use?

How do you maintain data lineage and provenance to ensure the integrity and traceability of your AI training data?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Access Control and Authentication:**

**Top-level question:** How will you control and manage access to your AI solution and its underlying components?

**Extra credit questions:**

What authentication and authorization mechanisms have you implemented to prevent unauthorized access?

How have you applied the principle of least privilege to ensure users and system components only have the minimum necessary permissions?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Monitoring, Logging, and Incident Response:**

**Top-level question:** How will you continuously monitor your AI solution for potential security incidents and respond to them?

**Extra credit questions:**

What monitoring and logging mechanisms have you put in place to detect anomalous behavior or potential security breaches?

Have you developed an incident response plan specific to your AI solution, and how will you test and refine it?

What incident response testing and drill procedures have you established to ensure your team is prepared to handle AI-related security incidents?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Secure Development and Testing:**

**Top-level question:** How have you incorporated security considerations throughout the development lifecycle of your AI solution?

**Extra credit questions:**

What secure coding practices and standards have you followed to minimize vulnerabilities in your AI system's codebase?

Have you conducted thorough security testing, including vulnerability scans, penetration testing, and red teaming exercises?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**AI-Specific Risks and Safeguards:**

**Top-level question:** How have you addressed AI-specific security risks, such as adversarial attacks, model poisoning, or unintended outputs?

**Extra credit questions:**

What measures have you taken to ensure your AI model is robust against adversarial examples and evasion attempts?

How have you implemented safeguards to detect and prevent model drift or unauthorized tampering with your AI system?

What techniques have you employed to enhance the interpretability and explainability of your AI model, and how does this contribute to its security?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Third-Party and Supply Chain Risk Management:**

Top-level question: How have you managed cybersecurity risks associated with third-party components or services used in your AI solution?

**Extra credit questions:**

Have you conducted vendor risk assessments and established security requirements for any third-party AI services or components?

What processes do you have in place to monitor and maintain the security posture of your AI solution's supply chain?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Compliance and Regulatory Considerations:**

**Top-level question:** How does your AI solution comply with relevant cybersecurity regulations and standards?

**Extra credit questions:**

Have you identified the specific cybersecurity regulations and standards applicable to your AI solution and its intended use case?

What measures have you taken to ensure compliance with these requirements, and how will you maintain compliance over time?

How do you keep up with evolving regulatory landscapes and adapt your AI solution's cybersecurity posture accordingly?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here:

**Ethics and Cybersecurity Alignment:**

**Top-level question:** How have you aligned your cybersecurity approach with the ethical considerations addressed in the ethics rubric?

**Extra credit questions:**

What steps have you taken to ensure your cybersecurity measures do not introduce or amplify ethical risks, such as privacy violations or bias?

How will you balance cybersecurity requirements with the need for transparency, fairness, and accountability in your AI solution?

**AI Disclosure:** If you have used AI tools to develop these answers, please disclose the service you used and the prompts you used here: