CYBER POSITION PAPER GUIDELINES

One of the best ways to prepare for any Model United Nations Conference is through researching for and writing a position paper. Not only will it give you a structured opportunity to become more acquainted with your committee's topic, but it will also allow you to fully flesh out your ideas and positions on the issues before the conference begins. While most BMUN committees follow a standard format, the U.S. Cybersecurity Committee (CYBER) will use a modified position paper structure to suit its specialized committee flow and topic.

Rather than including your country's position on a topic, as one would normally do in a position paper, your position paper should be divided up into **four** sections and will be based on which department you are representing in committee. These should be 5-10 pages in length, not including your works cited. The breakdown is as follows:

I. Profile of your Department **(10%)**
II. Proposals for Foreign Policy Revisions **(35%)**
III. Proposals for Domestic Policy Revisions **(35%)**
IV. Proposal for Personal Goals of your Department **(20%)**

***Percentages are section length suggestions. For example, for a 10 page paper the first section should be approximately 1 page.**

SUBMISSION INSTRUCTIONS

- You should have been emailed information for an account at huxley.bmun.org, specifically a username and password. If you do not have these, ask your advisor to reset your password (make sure the correct email is entered). A link labeled 'Position Paper' will appear next to where it says 'Profile'. Clicking on this will switch you to a page where you can then upload your paper for grading.

- Title your files Submission_Committee_Country
- If submitting your two position papers separately by topic, please indicate in the title as well using Topic1 or Topic 2 where appropriate
    - I.e. if you are in DISEC, and are representing Mauritania and submitting your position paper for topic 1, your file should be titled: Submission_DISEC_Mauritania_Topic1

Position Papers are due on **February 5th** to be considered for the ***Best Position Paper Award***, and **February 12th** to be considered for ***any committee award***. Late submissions will not be considered, and submissions will be graded on a rolling basis. It is advised that delegates submit their position paper when they are done instead of waiting till 23:59PST the day of the deadline to get it in, to avoid technical difficulties.

PLAGIARISM AND CITATIONS

All position papers will be extensively cross-referenced through various sources, both online and in-print. If there is any evidence of using the work of others without citations, the delegate(s) will not be eligible for an award. Any school that has multiple cases of plagiarism may be reconsidered for a School Delegation Award. It is the responsibility of the delegate and the advisor to ensure this does not happen.

Delegates must also remember to correctly cite sources, and papers without any cited sources will not be accepted. For more information on how to use in-text MLA citations, visit Purdue OWL.

I. Profile of your Department (10%)

In this section, you should outline the relevance of department to cybersecurity. We understand that some positions are more relevant to cybersecurity than others, this will be taken into account for position paper evaluation and committee evaluation. This is also why it is such a small part of your overall grade.

II. Proposals for Foreign Policy Revisions (35%)

For the Proposals for Foreign Policy Revisions, you should detail the changes to current American foreign policy which you believe would be useful to the advancement of the United States' cybersecurity goals and would enhance cybersecurity in the United States more generally. You should review the positions of the current administration, more generally and not of your department, and make any suggestions that you think would advance US cybersecurity. These can be soft power changes, hard power or militaristic changes, the creation of partnerships or alliances between countries, or really any levers that adjust or change the international position of the United States.

III. Proposals for Domestic Policy Revisions (35%)

This is your internal policy; basically, how will your department change its policies to adapt to the needs demanded by the current American cybersecurity infrastructure and threats to its security. How would you change the US government's policy to meet the needs of the cybersecurity situation? Lay those ideas out here. This should be overall, and not department specific.

IV. Proposal for Personal Goals of your Department (20%)

This is where you can dig into the specifics of your department's goals. You should be specific to the ideas you have about how you can leverage the capabilities of your department to enhance American cybersecurity and contribute to the goals outlined in the above sections. What do YOU contribute to this agenda that you've outlined above?

IMPORTANT CLARIFICATIONS ABOUT CYBER

Timeline **-** The first session of committee starts on March 2, 2018 in the Crisis Timeline. The way time progresses in committee will be revealed as committee events unfold.

Representation of Positions **-** You represent the head of your department, however you are *not that person specifically*. For example for the Federal Bureau of Investigation, the person represented is **not** *Cristopher Wray*, but rather the *Director of the FBI*. Any position still retains the full portfolio powers of their department (within reason of course). This is because I rather you focus on the role rather than researching the history of a particular person. This also means that your portfolio powers should be focussed on expanding the powers and range of actions of your department, rather than a particular person.

List of Positions **-** For the sake of transparency, I have included a list of all positions at the bottom of this document. These are all the potential positions, not all of them will necessarily be represented in committee.

I understand that this may be unclear/irregular. Crisis committee always are in my experience. If you have any questions, I highly encourage you to email your questions to jtibbetts@bmun.org. I will try to update this document with future clarifications based on your questions.

LIST OF COMMITTEE POSITIONS IN CYBER

This list is a comprehensive description of the representatives who will be present in the committee. This should help you better understand who and what you'll represent in committee

Position	Description
Head of Strategic Intelligence	Long Term Intelligence Planning
Head of Operational Intelligence	Offensive Operations
Head of Counterintelligence	Defensive Operations
Head of Tactical Intelligence	Analyzing and Supporting Intelligence and Operations
Air Force Cyber Command Liaison	Represents the Air Force
Army Cyber Command Liaison	Represents the Army
10th Fleet Command Liaison	Represents the Navy
Marine Corps Cyberspace Command Liaison	Represents the Marines
US Space Command Liaison	Represents US Space Command
NSA Intelligence Liaison	Represents the NSA
CIA Intelligence Liaison	Represents the CIA
FBI Intelligence Liaison	Represents the FBI
Secret Service Intelligence Liaison	Represents the Secret Service
Department of Energy Liaison	Represents the Department of Energy
DISA Intelligence Liaison	Represents the Defense Information Systems Agency
Department of Defense Liaison	Represents the Department of Defense
Department of Homeland Security Liaison	Represents the Department of Homeland Security
Department of State Liaison	Represents the Department of State
Department of Transportation Liaison	Represents the Department of Transportation

Department of Treasury Liaison	Represents the Department of Treasury
Special Advisor to the President on Cybersecurity (Cyber Czar)	Represents the interests of the executive branch
US Strategic Command Representative	Provides Integration of this committee into broader military network
Representative of Congressional Cybersecurity Caucus	Congressional representative in committee
Department of Justice Liaison	Represents DoJ, helps provide legal grounds and advice for policymaking and crisis response