# PIT-UN Supplementary Grant Report

# Prepared by The MIT Cybersecurity Clinic

Lawrence Susskind[a], Jungwoo Chun[b] and Avital Baral[c]

December 27, 2021

[a] Dr. Lawrence Susskind is Ford Professor of Urban and Environmental Planning at MIT, Vice-Chair of the Program on Negotiation at Harvard Law School, Director of the MIT Science Impact Collaborative and Director of the MIT Cybersecurity Clinic.

[b] Mr. Jungwoo Chun is a doctoral candidate in the Department of Urban Studies and Planning at MIT and holds an MS degree from Fletcher School of Diplomacy at Tufts University and has served as Program Director of the Cybersecurity Clinic at MIT.

[c] Ms. Avital Baral completed her SB at MIT and her MS in Mechanical Engineering at MIT. She was one of the first students to participate in the Cybersecurity Clinic at MIT.

# Appendix (Course Syllabus, Fall 2021)

## 11.074/11.274 The MIT Cybersecurity Clinic

**Cybersecurity for Critical Urban Infrastructure**
**Course Syllabus Fall 2021, credits: 2-4-6**

**Professor: Lawrence Susskind**
**Office Hours: By Appointment**

**TA: David Hong**
**Office Hours: Please Email**

**Online Modules: edX/MITx**
**Mandatory In-Class Meetings (9-450A): Fridays, 10:00AM-12:00PM**
**First Class: 9/10/2021**

The Cybersecurity Clinic is a semester-long course that begins with four, one-week instructional modules. These interactive sessions require 2-3 hours a week of online preparation along with an in-class discussion each Friday from 10 a.m. – noon. The Friday in-class discussions will run the full length of the course, while the online instructional modules must be completed within the first four weeks between September 10 and October 8, 2021.

**Course modules cover:**

1) Cybersecurity for Critical Urban Infrastructure: Understanding the Problem;
2) How the MIT Cybersecurity Clinic Makes Initial Contact with potential Client Agencies;
3) Onsite Assessment of Cybersecurity Vulnerability by MIT Clinic Staff; and
4) Preparing and Submitting a Cybersecurity Vulnerability Assessment to a Client Agency.

MIT or Harvard students seeking field assignments with the Cybersecurity Clinic (for academic credit) must pass the 20 question online multiple-choice certification examination at the end of the fourth module.

The Clinic provides an opportunity for MIT students to become certified in methods of assessing the vulnerability of public agencies (particularly agencies that manage critical urban infrastructure) and hospitals to the risk of cyberattack. Certified students will work in teams with client agencies and hospitals in various cities and towns around the United States. Through preparatory interactions with client agencies and hospitals, and short on-site visits, student teams will prepare Vulnerability Assessments that client agencies and hospitals can use to secure the technical assistance and financial support they need to manage the risks of cyberattack they are facing.

### Student Expectations

#### Inclusive Classroom

MIT values an inclusive environment. We hope to foster a sense of community in this class and consider this class to be a place where you will be treated with respect. We welcome individuals of all backgrounds, beliefs, ethnicities, national origins, gender identities, sexual orientations, religious and political affiliations – and other visible and nonvisible differences. All members of this class are expected to contribute to a respectful, welcoming, and inclusive environment for every other member of the class. If this standard is not being upheld, please let us know.

## Adherence to MIT's Academic Regulations

This syllabus has been developed, and this class will be conducted, in full adherence to the MIT Academic Policy and Regulation Team (APART) policies and the Grading Policy.
Other term regulations and examination policies remain in effect.

## Academic Integrity

You are encouraged to learn from one another in this class. You may collaborate with class members while participating in the field assignment component of the course, but the certification exam at the end of the online learning modules should be your own work, independent of any collaboration. For questions arising from online modules, please contact the TA for clarification. The MIT Policy on Student Academic Dishonesty is outlined in MIT's Policies and Procedures 10.2.

Violating the Academic Integrity policy in any way may result in receiving a failing grade on the course, having a formal notation of disciplinary action placed on your MIT record, suspension from the Institute, and expulsion from the Institute for very serious cases. Please review MIT's Academic Integrity policy and related resources (e.g., working under pressure; how to paraphrase, summarize, and quote; etc.) and contact Larry or David if you have any questions about appropriate citation methods, degree of collaboration permitted, or anything else related to academic integrity.

## Learning Norms

You are expected to attend the weekly Friday classes, which will include discussions on instructional modules, readings, lectures by guest speakers, and preparation and debriefs for the field exercise. If for some reason you are unable to attend, please discuss with the TA in advance. It is your responsibility to figure out what you missed — including any changes to the syllabus and assignments, or other important announcements.

## Assignments and Grading

The target for the course is for you to learn how to identify, evaluate, and communicate gaps within an organization's cybersecurity program and to propose corresponding improvements.

While this course follows a Pass/ No Record structure, below are the requirements for you to succeed and obtain a passing grade. Note that Pass reflects performance at levels of A, B, and C. Please see the Grading section of MIT's Rules and Regulations for additional guidance. Please take note that there will be no final exam for this course during the December exam period. For further clarifications, please contact the TA.

| Items | Requirements | Relative % |
|---|---|---|
| 1. Certification Exam | 80% or higher on multiple choice on Edx online learning modules (20 questions) by Oct 7 | Required to pass course |
| 2. Field Assignment | Submission of final report by Dec 3 | 50% |
| 3. Class Participation | Attendance and active participation in Friday class discussions | 50% |

**1. Certification Exam**

I. 2 Parts, 20 questions total, multiple choice

II. Analysis of video simulation with multiple choice questions as well as questions based on course readings

III. You must achieve a score of **80% or higher to pass the course and get your certificate.**

IV. There will be one attempt provided, and we fully expect you to achieve a passing grade or higher by the end of all the modules.

V. The deadline to take the Edx certification exam is by **11:59 PM EST Thursday, October 7**. We encourage you to take it before that time in case of any system errors.

**2. Field Assignment (10/8- 12/9):**

I. Once students have achieved certification, they will be assigned to teams. Each team will help a public agency or hospital prepare a Cyberattack Vulnerability Assessment. (Students will learn what they need to know to prepare such Assessments by completing the four online modules).

**3. Class Participation**

I. Evaluation of participation will be a function of attendance as well as engaged conversation. We firmly believe that each and every one of you have valuable insight to contribute, but we are also mindful of cultural differences when it comes to speaking up. All of this will be taken into consideration.

II. Much of your in-class learning will come from exchange and collaboration in small groups of your own peers. Therefore, attendance is mandatory – barring any Institute changes to pandemic response.

III. In the event of a personal emergency, please send an email to the TA for accommodation [ahead of time whenever possible]. No more than two (2) absences are advised to receive a passing grade for the participation portion. For any exceptions, please contact the TA.

**<u>Special Accommodations</u>**

MIT is committed to the principle of equal access. Students who need disability accommodations are encouraged to speak with Disability and Access Services (DAS), prior to or early in the semester so that accommodation requests can be evaluated and addressed in a timely fashion. If you have a disability and are not planning to use accommodations, it is still recommended that you meet with DAS staff to familiarize yourself with their services and resources. Please visit the DAS website for contact information.

If you have already been approved for accommodations, class staff are ready to assist with implementation. Please inform Professor Susskind AND David Hong (hongdav@mit.edu) who will oversee accommodation implementation for this course.

## Student Support

### Undergraduate Students: Student Support Services (S3)

If you are dealing with a personal or medical issue that is impacting your ability to attend class, complete work, or take an exam, you should contact a dean in Student Support Services (S3). S3 is here to help you. The deans will verify your situation, provide you with support, and help you work with your professor or instructor to determine next steps. In most circumstances, you will not be excused from coursework without verification from a dean. Please visit the S3 website for contact information and more ways that they can provide support.

*Website: https://studentlife.mit.edu/s3*

### Graduate Students: GradSupport

As a graduate student, a variety of issues may impact your academic career including faculty/student relationships, funding, and interpersonal concerns. In the Office of Graduate Education (OGE), GradSupport provides consultation, coaching, and advocacy to graduate students on matters related to academic and life challenges. If you are dealing with an issue that is impacting your ability to attend class, complete work, or take an exam, you may contact GradSupport by email at gradsupport@mit.edu or via phone at (617) 253-4860.

### Mental Health

Many of us face issues with our mental health over the course of our lives, and sometimes being a student can create or exacerbate these issues. If you are struggling, your mental health is suffering, or you just need someone to talk to, we encourage you to make an appointment with Student Mental Health and Counseling Services by calling 617-253-2916 or visiting https://medical.mit.edu/services/mental-health-counseling. Please don’t wait until you reach a state of crisis to ask for help. It’s hard to do, but important. These services are free and confidential.

## Course Schedule

Tentative – may change slightly as we set up the pace of the class and on guest speaker availability

How to read the table below: The first date under the 'Dates' column marks the Friday meeting session (e.g., 09/10). This date corresponds with the lecture activity that will take place on that day. The 6-day period under the 'Dates' column (e.g., 09/10 - 09/16) is linked with the time you have to carry out items in the 'Student Activity' column.

| Week | Dates | Module/ Lecture Activity | Student Activity | Deadline |
|---|---|---|---|---|
| 1 | 09/10 – 09/16 | Course Introduction, Overview, and Expectations | Complete Edx Module 1 and assigned readings by week 2 | - |
| 2 | 09/17 – 09/23 | Discussion of Edx Module 1 - Understanding the Cybersecurity Problem | Complete Edx Module 2 and assigned readings | - |
| 3 | 09/24 – 09/31 | Discussion of Edx Module 2 - Initial Communications with a Client Agency | Complete Edx Module 3 and assigned readings | - |
| 4 | 10/01 – 10/07 | Discussion of Edx Module 3 - Onsite Assessment of Cybersecurity Vulnerabilities | Complete Edx Module 4 and assigned readings<br>**- Take the Certification Exam on Edx** | **Certification Exam** - Due: **October 7** at 11:59 PM |
| 5 | 10/08 – 10/14 | Discussion of Edx Module 4 - Preparing a Cybersecurity Vulnerability Assessment<br>**Group Discussion:** Planning Client Assessments + How to sequence interviews (e.g., based on complexity and stakeholder importance) | - Field Teams are assigned<br>- Send out client communication requesting:<br>- Point of contact<br>- Planning call for interview scheduling. Desired Output: interview dates/ times<br>- Questionnaire to be filled<br>- Date: when questionnaire will be completed and sent back | - |
| 6 | 10/15 – 10/21 | **Lecture:** Philip Mah on Challenges and Approaches of Securing Cyber-Physical Systems<br>**Group Discussion:** Discuss responses from client and how scheduling is progressing. | - Begin analysis on questionnaire responses - Schedule interviews<br>- How to collect positive observation early on<br>- Rehearse interviews and prepare to gather information to populate the final report | - |
| 7 | 10/22 – 10/28 | **Lecture:** Manish Khera on the Importance of Protecting Critical Infrastructure (Power Grid Perspective)<br>**Group Discussion:** Client Interviews | - Begin interviews<br>- Analyze questionnaire responses and interview responses, and see where additional interviews are needed<br>- Schedule any additional interviews and request any remaining information | - |

|  |  |  |  |  |
|---|---|---|---|---|
| 8 | 10/29 – 11/04 | **Lecture:** Abhishek Nandawat on Vulnerability and Threat Management<br>**Group Discussion:** Discuss progress on interviews, prepare analysis for reporting, identify potential gaps in reporting and devise solutions | - Continue and finalize interviews<br>- Structure the assessment report and begin outlining outputs | - |
| 9 | 11/05 – 11/11 | **Lecture:** Danny Weitzner on US Efforts to Improve the Cybersecurity of Critical Infrastructure Sectors<br>**Group Discussion:** Report writing, including tone | - Write the Draft Assessment | **Submit Draft Assessment** to the TA (Nov 11) |
| 10 | 11/12 – 11/18 | **Group Discussion:** Share Draft Assessment with peers, review, and discuss | - Share your Draft Assessment with another group and discuss<br>- Take note of feedback received and consider which comments to incorporate<br>- Schedule any feedback gathering session with client in advance of sending the Draft Assessment | - |
| 11 | 11/19 – 11/24 | **Group Discussion:** Present Executive Summaries and Receive In-Class Feedback before Draft Submission to Client Contact | - Review TA comments and make revisions as needed<br>- Continue to discuss Draft Assessment and make revisions<br>- Draft finalize the assessment and share with the client. When sending to the client, schedule a call to confirm client feedback (This call is to receive it verbally if they have not provided it by the agreed date, but also to be clear on what was meant in their comments) | **Submit Draft Assessment to client** for their feedback (Nov 22) + Ask for any client feedback by Nov 30 and schedule a review call for Nov 30 |
| 12 | 11/26 | Thanksgiving Holiday (No class) | Rest | - |
| 13 | 12/03 – 12/09 | **Group Discussion:** Debrief on Client Feedback and Compare Findings + Class wrap up | - Share client feedback received with the class for discussion<br>- Internally review Final Assessment<br>- Finalize the Assessment | **Submit Final Assessment electronically to client** (Dec 7)<br><br>**Address any final feedback** by client if received and share back revised copy (Dec 9). Thank them for their participation |

**Return to in-person teaching/learning**

MIT and DUSP are excited at the opportunity for a return to in-person teaching and learning after 2+ semesters of remote life. To ensure that all classes can and will be delivered in person, MIT has worked hard to put into place policies, procedures, and technologies to maximize the likelihood of a safe and uninterrupted semester.

That said, the ever-evolving pandemic means we need to be prepared. If any student in class tests positive for covid-19, MIT Medical has established clear procedures for ensuring safety of everyone and MIT's Class Notification and Support Team will help that student continue learning to with the least possible disruption. If any of the instructors in this class are unable to attend in person due to covid-19, we will work together with the leadership of DUSP, the School, and the Institute to ensure minimum disruption.

In the case of the need for any remote teaching, we will use this "zoom classroom": https://mit.zoom.us/j/94157394623

**Online Module Contents + Readings <note there are more readings below than in Edx>**

**Module 1: Cybersecurity for Critical Urban Infrastructure: Understanding the Problem**

I. The Scope of the Cybersecurity Problem Facing American Cities
II. Lines of Cyber Attack
III. The Federal Government's Response to Cyber Attacks
IV. Who are the attackers?
V. The Baltimore Case Study – Parts 1 & 2
VI. Key Take-Aways from Module 1

**Readings (Due: Sept 16 before Sept 17 meeting)**

- Fernandez, Manny et al. (2019). 'Ransomware Attacks are Testing the Resolve of Cities Across America', New York Times, 22 August.
- Assante, Michael, and Andrew Bochman. (2017), 'Automation, Autonomy & Megacities 2025: A Dark Preview', Center for Strategic and International Studies 3.
- 'Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks' Whitehouse.gov. (2021)

**Module 2: The MIT Cybersecurity Clinic's Initial Communications with a Client Agency**

I. The MIT Cybersecurity Clinic and its Mission
    A. Checklist
    B. Letter of Agreement
II. What is a Vulnerability Assessment?
III. Initial Questions to Ask and Answer
    A. Initial questionnaire
IV. Reviewing the Information Provided by A Client Agency
    A. Initial questionnaire

V. Simulation 1: An Unsuccessful Initial Conversation with a City Agency
Simulation 1 Debrief

VI. Simulation 2: A successful Initial Conversation with a City Agency
Simulation 2 Debrief

VII. Key Take-Aways from Module 2

**Readings (Due: Sept 23 before Sept 24 meeting)**

- Cohen, Natasha and Nussbaum, Brian (2018), 'Cybersecurity for the States: Lessons from Across America,' *New America Foundation*. Please read CH 1, 2, 3 inclusively.
- Falco, Greg et al. (2019), 'Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks', *Journal of Cyber Policy*.
- Huang, Keman and Pearlson, Keri (2019), 'Being a Model of Organizational Cybersecurity Culture', Cybersecurity at MIT Sloan.

**Module 3: Onsite Assessment of Cybersecurity Vulnerabilities**

I. Collecting Information Onsite for the Vulnerability Assessment
    A. Onsite questions

II. Conducting Onsite Interviews
    A. Onsite questions

III. Simulation: An Unsuccessful Effort to Gather More Information
Debrief

IV. Simulation: A Successful Effort to Gather More Information
Debrief

V. Key Take-Aways from Module 3

**Readings (Due: 09/31 before 10/01 meeting)**

- Stauffer, Nancy (2019), 'Protecting our Energy Infrastructure: New Analysis Targets Cybersafety', *Energy Futures*, Spring 2019.
- Dudley, Renee (2019), 'The Extortion Economy: How Insurance Companies are Fueling a Rise in Ransomware Attacks' *ProPublica*, 27 August.
- Monroe, Rachel (2021), 'How to Negotiate with Ransomware Hackers', The New Yorker, 31 May.

**Module 4: Preparing A Cybersecurity Vulnerability Assessment**

I. Considerations in Preparing a Vulnerability Assessment

II. What Needs to Be Covered in an Assessment?
    A. Draft Vulnerability Assessment

III. Simulation: An Unsuccessful Effort by Clinic Staff to Complete a Draft Assessment
Debrief

IV. Simulation: A Successful Effort By Clinic Staff to Complete a Draft Assessment Debrief

V. Anticipating Agency Concerns About the Draft Assessment
    A. Draft Vulnerability Assessment

VI. Simulation: An Unsuccessful Effort to Present a Draft Assessment Debrief
VII. Simulation: A Successful Effort to Present a Draft Assessment Debrief
VIII. Standards of Care
IX. Key Take-Aways Moving from Module 4

**Conclusion**

I. Final Course Take-Aways
II. Instructions for Certification Exam

**Module 5:** Challenges and Approaches of Securing Cyber-Physical Systems
**Reading (Due: 10/14 before 10/15 guest lecture)**

- Ivezic, Marin (2015), 'The World of Cyber-Physical Systems & Rising Cyber-Kinetic Risks,' 5G Security, 31 March.

**Module 8:** US Efforts to Improve the Cybersecurity of Critical Infrastructure Sectors
**Reading (Due: 11/04 before 11/05 guest lecture)**

- 'NIST Cybersecurity Framework Online Learning,' NIST.gov. < https://www.nist.gov/cyberframework/online-learning>. Please read all subsections of this page except Introduction to Framework Roadmap, and Update Process.