Professor Catherine Chatfield

cchatfield@alaska.edu

Tools for Success

HSEM F434 All Hazards Risk Analysis

Introduction

Given that on-line teaching can sometimes assume that all students are starting with the same foundational knowledge, this toolkit will help those who may not have been introduced to these concepts in the past and may need a bit more foundational instruction other than outlined in the individual unit objectives.

This document will provide helpful hints on how to fully engage with the class. Some of these are skills in accessing the tools you need, while some will teach you skills on how to implement the assignments with the least amount of effort – a win-win for both the student and the teacher!

Feel free to suggest additional sections for this manual through your exit surveys, an email or DM to me on Slack.

I look forward to learning with you!

Catherine

Table of Contents

[Accessing your Slack Account 2](#_Toc24290842)

[Use an invitation to access the Slack Site 2](#_Toc24290843)

[Search for the course on Slack.com 3](#_Toc24290844)

[Ask the Slack Administrator add you directly 4](#_Toc24290845)

[How to successfully complete the Decision Brief Series 6](#_Toc24290846)

[Overview 6](#_Toc24290847)

[Your checklist for success 7](#_Toc24290848)

[How to identify Critical Infrastructure & complete Vulnerability Analyses 9](#_Toc24290849)

[Overview 9](#_Toc24290850)

[Identifying Critical Infrastructure 9](#_Toc24290851)

[Completing a vulnerability analysis 11](#_Toc24290852)

# Accessing your Slack Account

This course will have a dedicated Slack site for weekly communications. This platform replaces the use of Blackboard Discussion Boards and will generally focus on various aspects of Risk Communication. There are multiple ways in which a student can access their Slack account.

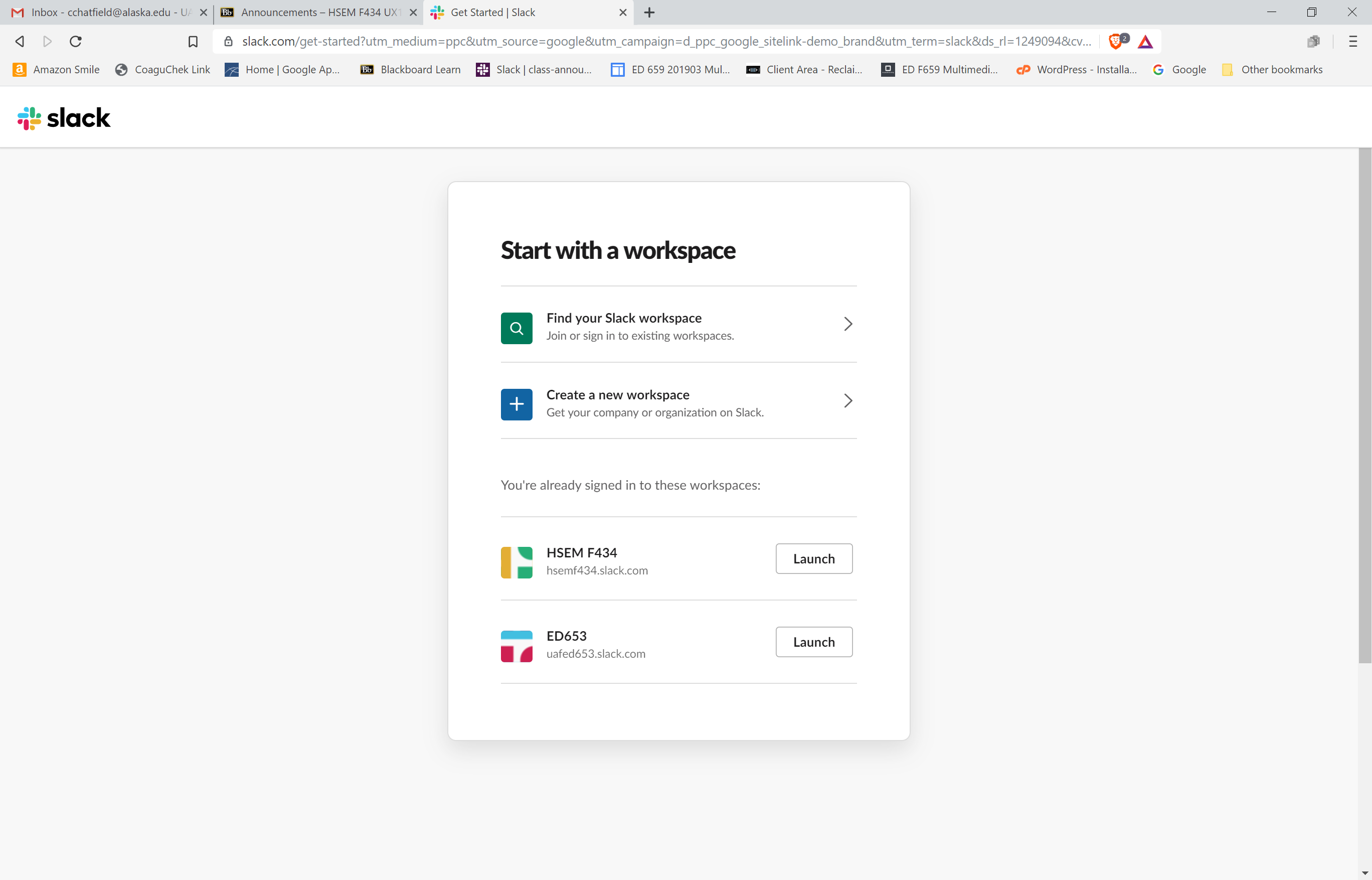
There are multiple ways in which to access your account – Use the invitation as provided in your welcome announcement, search for the course direction on Slack or, as a last resort, ask the Slack administrator (that would be me) to invite you. Here’s what each of these looks like.

## Use an invitation to access the Slack Site

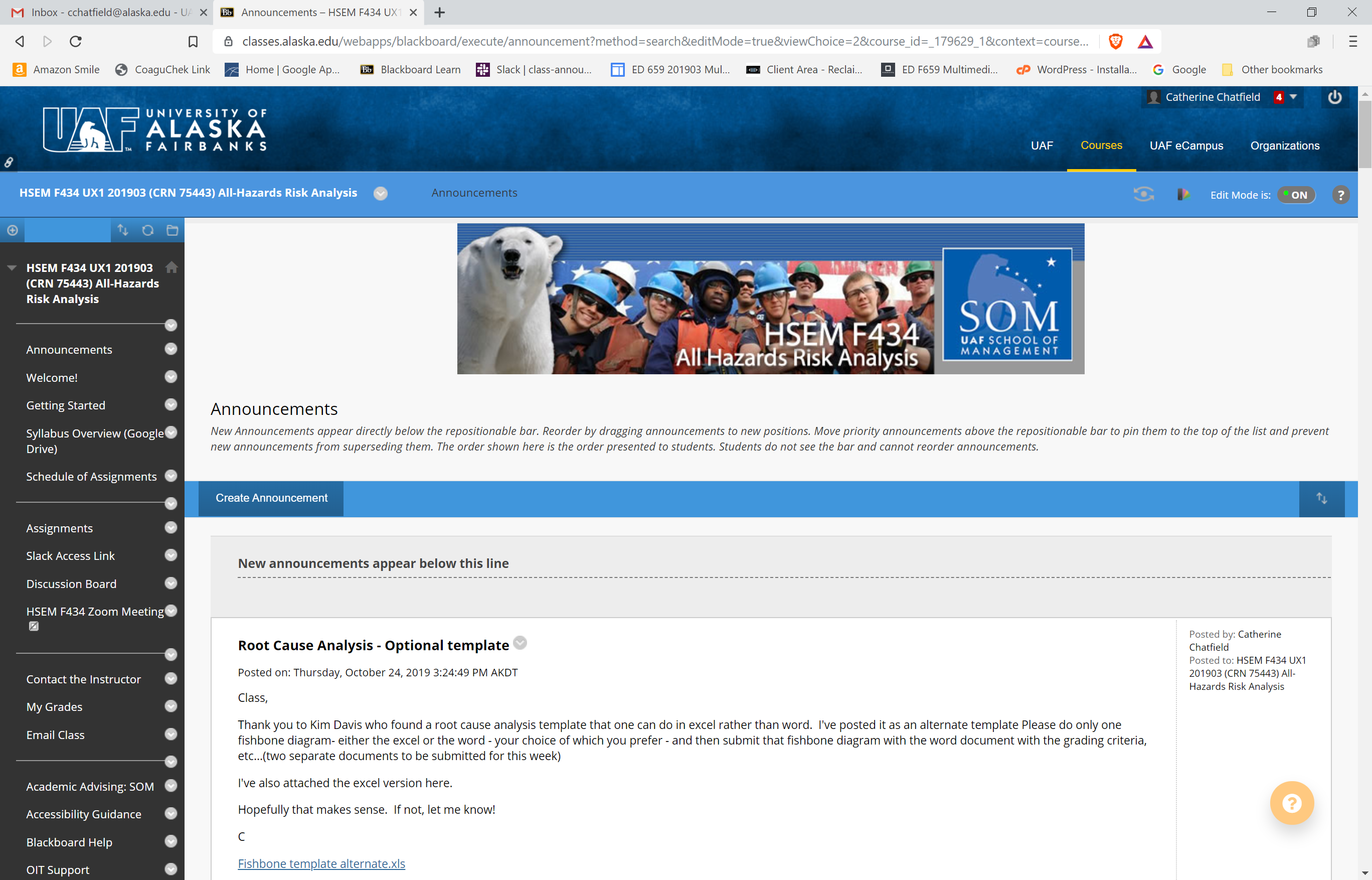
At the beginning of class, I will send an email with an active link that looks something like this:

[https://join.slack.com/t/hsemf434/signup](https://join.slack.com/t/hsemf434/signup?x=x-p714147973047-700883336450-733414593795)

*Note: please don’t use this specific link as there will be a different sign up for each semester’s class*

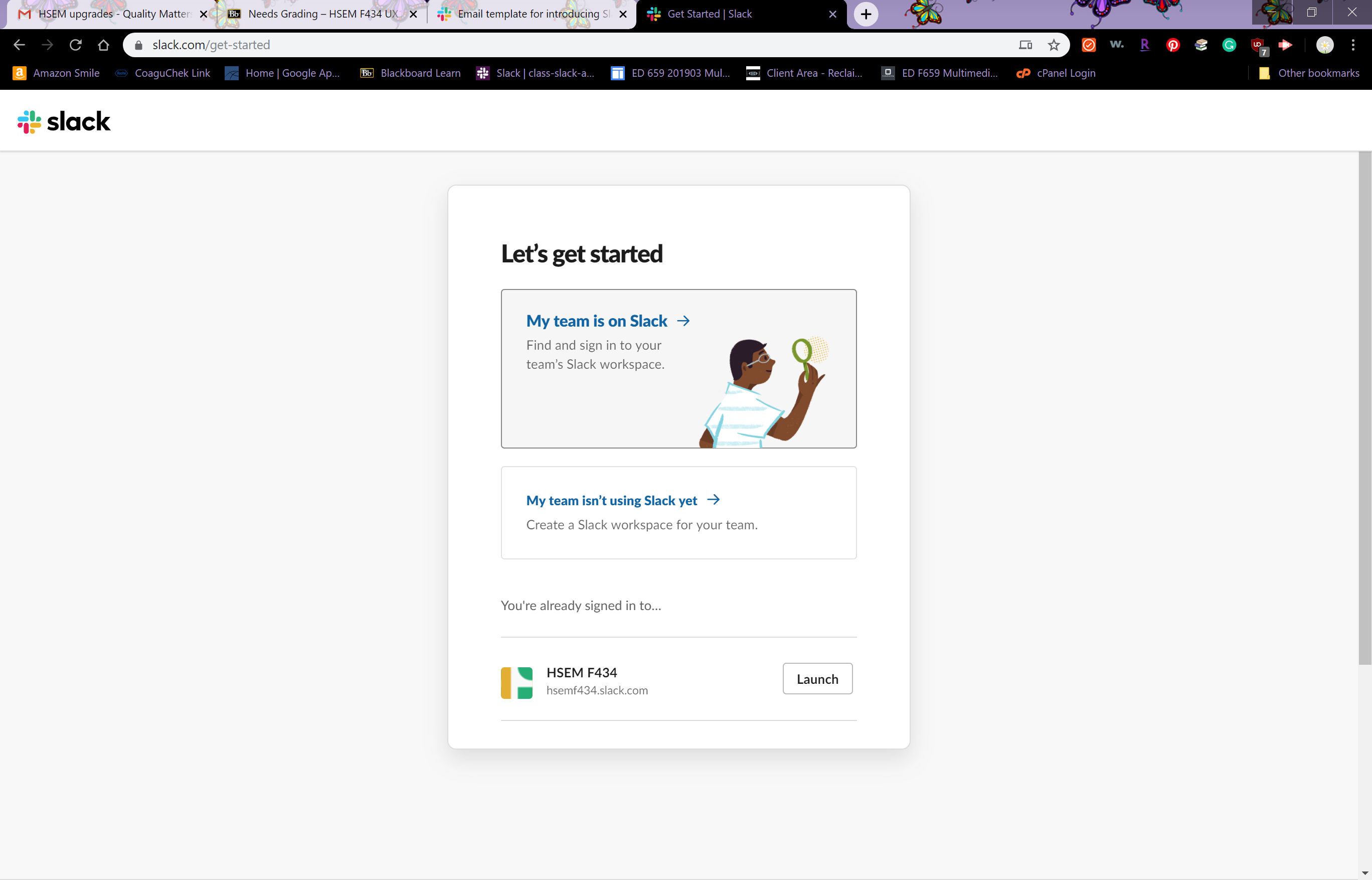


On Blackboard, I’ll have a link to the risk communication channel where you’ll be posting your required assignments:

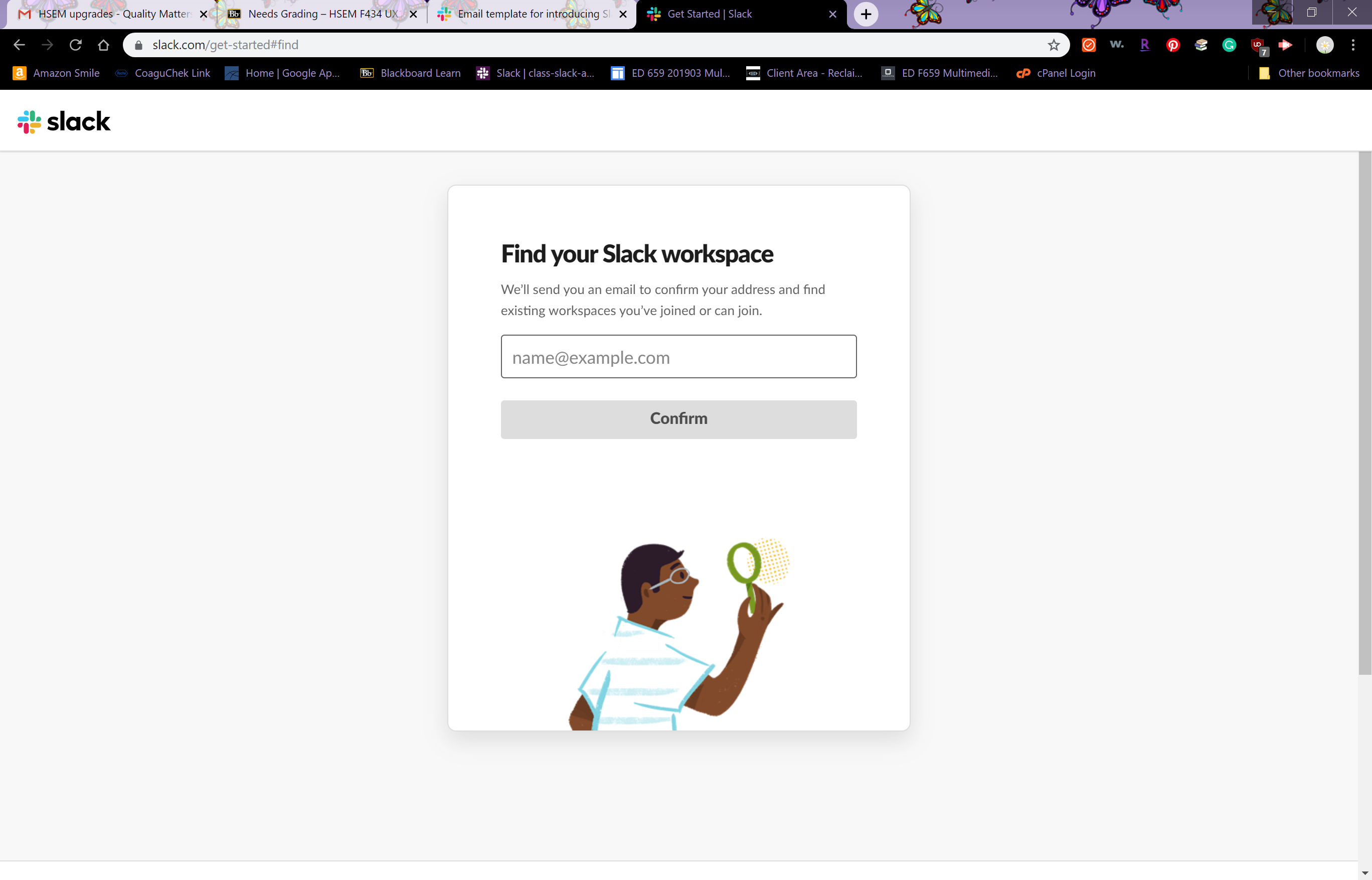


## Search for the course on Slack.com

If you don’t have an invite or the invite isn’t working, then click on [**https://slack.com/get-started**](https://slack.com/get-started) and click “My team is on Slack”



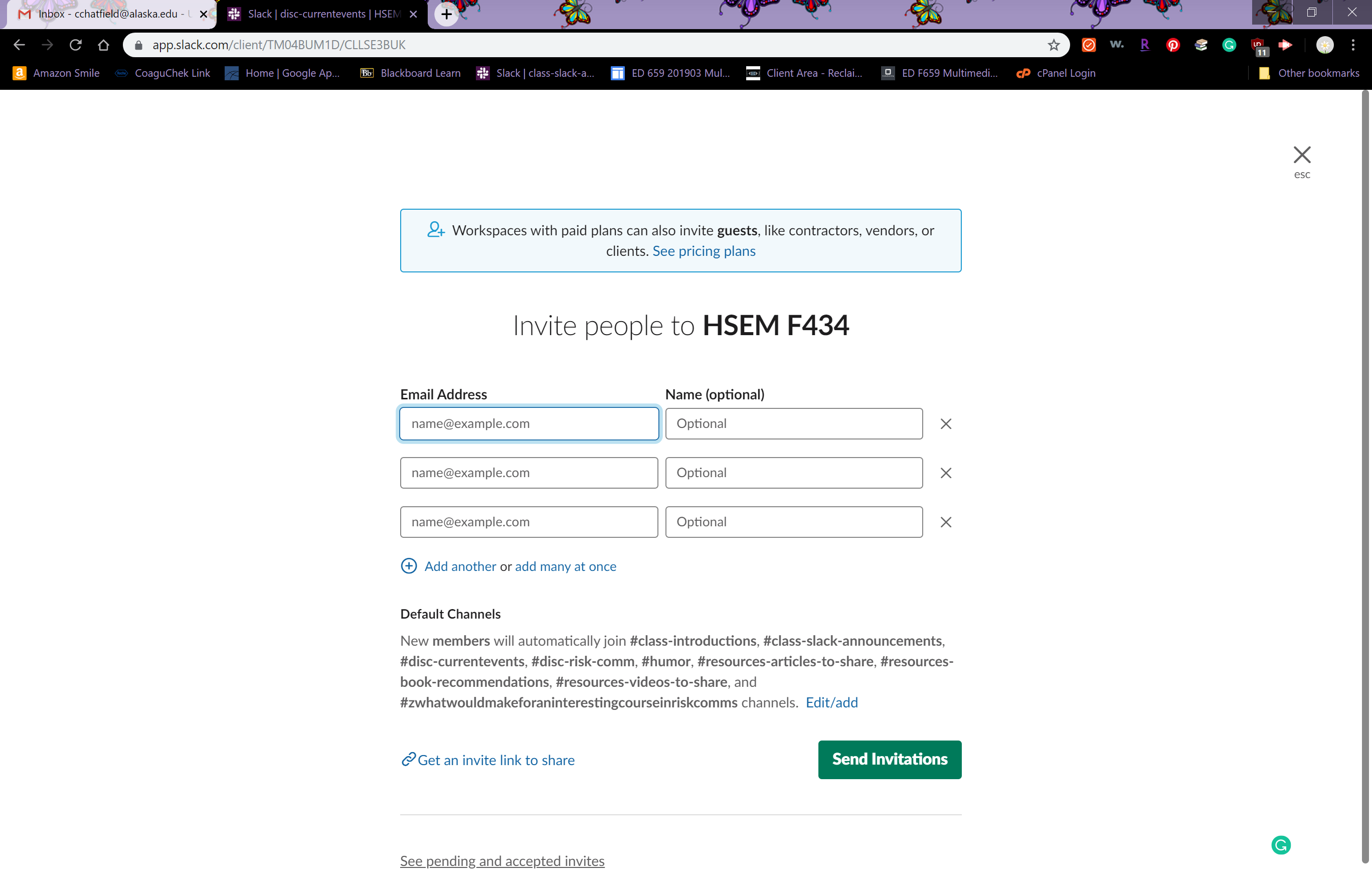
You should then see this option:



Enter your email address and select the Slack workspace associated with this class

## Ask the Slack Administrator add you directly

Lastly, the administrator can add you directly, although she might be disinclined to do that for an extremely large class!



Now that you’re in, you can routinely access your site through the following methods:

* Slack.com
* Through Blackboard
* Through your mobile device. You can download Slack to your phone.
* [Download Slack for Android](https://slack.com/help/articles/207691318-download-slack-for-android)
* [Download Slack for iOS](https://slack.com/help/articles/208401947-Download-Slack-for-iOS)

Make sure you bookmark this site as you’ll be going to it periodically.

And if you’re not familiar with Slack, you can review the tips posted by your administrator and the tips contained in Slack’s [Getting Started](https://slack.com/help/categories/360000049043#intro-to-slack) guidance.

# How to successfully complete the Decision Brief Series

## Overview

This is a series of 7 exercises that culminate in a decision brief. The decision brief is intended to be for the stakeholders in your community. This set of exercises is the foundation of the course and students should focus on understanding how the pieces of the puzzle come together. All other assignments are intended to reinforce these specific set of activities.

As shown in the opening set of slides, the DHS Risk Management Framework as detailed in Figure 1 is a function of the Hazard/Threat, the Vulnerability and the Consequences to a given target.

A screenshot of a cell phone

Description automatically generated

Figure The DHS Risk Management Framework

Your Decision Brief will be developed to be presented to the stakeholders you develop in the first exercise. It may be helpful to think about your decision brief as answering the following questions:

1. Who are the stakeholders?
2. Where is the target and what are the vulnerabilities to that target?
3. What risks will the target face (based on the likelihood and consequences that you select)
4. How can these risks be better managed (mitigation strategies)?

Focus your data collection on the TARGET infrastructure and not the town, state or country where the target resides. Select your target with enough information to conduct the risk assessment. If you can’t find data for your town, find data for a similar event in a different part of the country and extrapolate whether or not the data is applicable or not and why.

Figure 2 shows the individual steps that will need to be completed in order to deliver your decision brief.

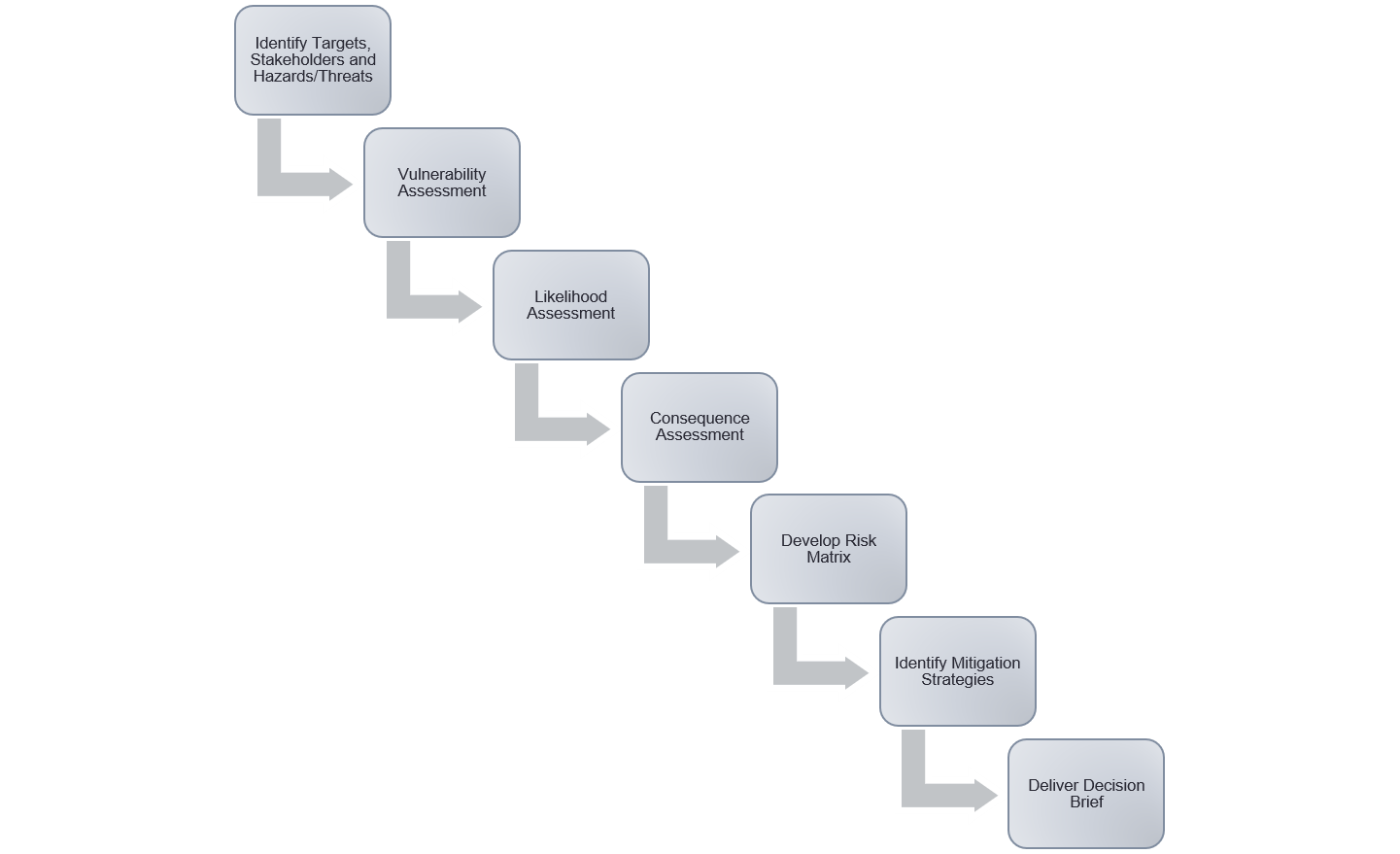


Figure : The Decision Brief Series

## Your checklist for success

* Each exercise assignment has prescribed format and content requirements as well as the grading rubrics.  Please follow the instructions carefully.
* You must use the template provided and submit as either a Microsoft Word or PDF document. If I can’t read it in Blackboard, I’ll mark it with a “0” and send it back. Students who don’t currently own Microsoft Word should know that they have access to this as a student. Contact the OIT help desk for guidance on how to access Microsoft 365.
* Label all exercises as follows: **Year\_month\_date\_name of exercise\_your first initial\_your last name:** i.e. 2019\_09\_01\_Threat Assessment\_C\_Chatfield
* Failing to label your exercises or include your name on your submitted document results in an automatic reduction - n of points, as I download these to follow the evolution of your project.
* Please give credit where appropriate for all sources, including photos. When required, full citations must be provided for full credit. You are not writing for you or for me – you are writing for the client who can’t get inside your head to know where you’ve been. You must include the complete URL. Leave a few breadcrumbs as you will lose points if I can’t find the same reference that you’re using or if the reference is not representative of the question being asked.
* Decision Brief Assignment #1 (Critical infrastructure and hazards) must be completed before I grade any sequential assignments. If you submit assignments out of order, I will assign a value of 0 until the preceding assignment is received and graded. Late fees may be assigned as well.
* All Decision Brief Assignments must be completed in order. I will not grade assignments out of order nor will I will grade the final presentation until all previous assignments have been submitted.
* While you may change your hazards and threats based on what you learn during your analysis, you must keep those threats in the same order as originally presented. I don’t have time to do the gap analysis. Consistency will be key to success on these assignments.
* If one or more students are working on the same town, I will expect that they will develop separate hazards, threats and targets to minimize any perception of plagiarism.
* Begin with the end in mind. There are a couple of example decision briefs at the end of the course that can be used to help frame your thinking as well as the metrics that will be used to gauge your success in answering the questions above.

# How to identify Critical Infrastructure & complete Vulnerability Analyses

## Overview

In the first decision brief assignment, you will be asked to identify your town of interest as well as at least 10 different examples of critical infrastructure. The concept of critical infrastructure applies whether one is dealing with a large city or small town. Guidance on critical infrastructure was previously provided by FEMA and is now provided by CISA.

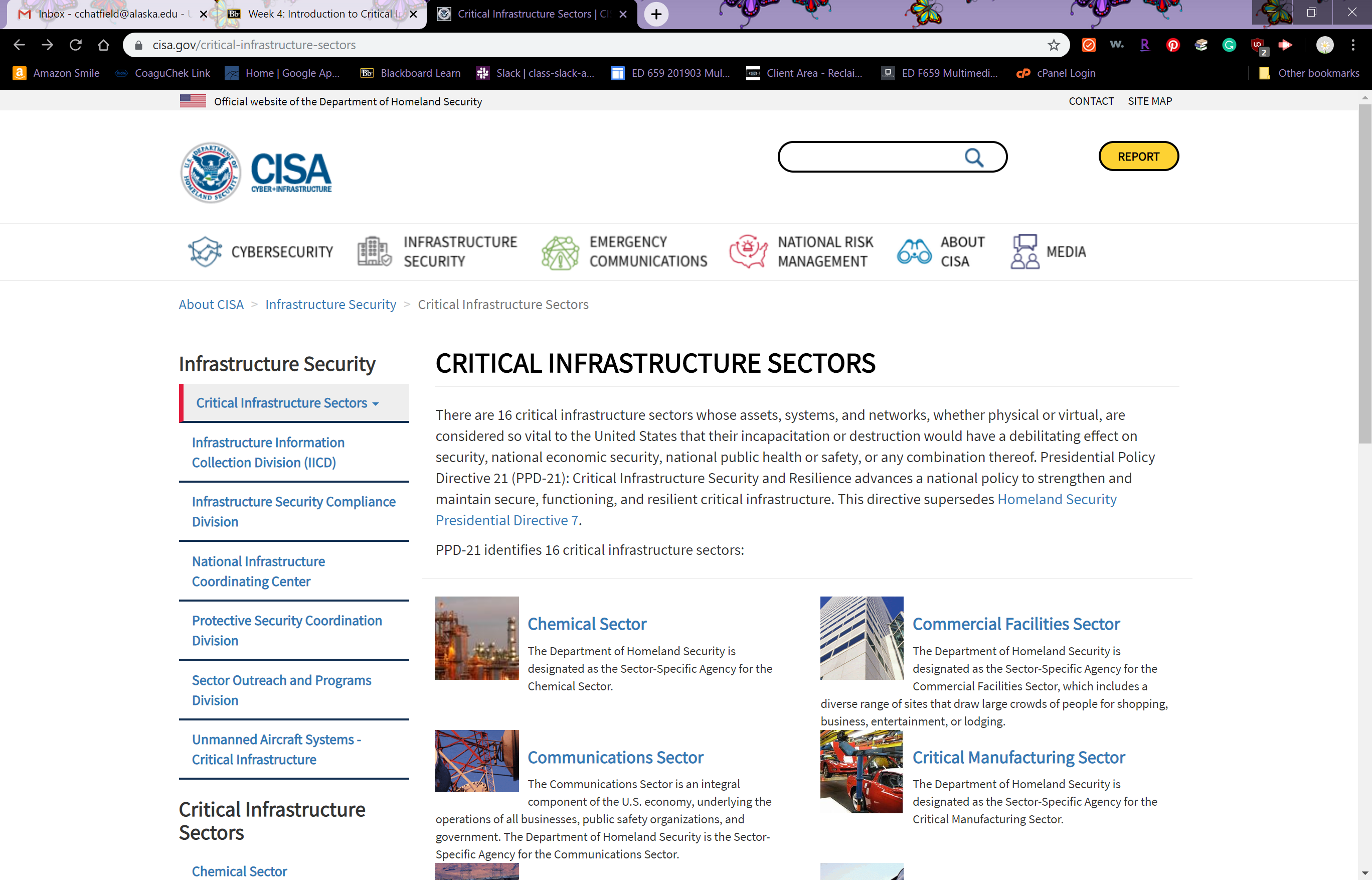
As background, the “**Cybersecurity and Infrastructure Security Agency** (**CISA**) was established on 16 November 2018 when [President](https://en.wikipedia.org/wiki/President_of_the_United_States) [Donald Trump](https://en.wikipedia.org/wiki/Donald_Trump) signed into law the [Cybersecurity and Infrastructure Security Agency Act of 2018](https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency_Act_of_2018).[[2]](https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency#cite_note-aboutcisa-2)[[3]](https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency#cite_note-zdnet-3) CISA is a standalone [United States federal agency](https://en.wikipedia.org/wiki/List_of_federal_agencies_in_the_United_States), an operational component under [Department of Homeland Security](https://en.wikipedia.org/wiki/Department_of_Homeland_Security) (DHS) oversight.[[3]](https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency#cite_note-zdnet-3) Its activities are a continuation of the [National Protection and Programs Directorate](https://en.wikipedia.org/wiki/National_Protection_and_Programs_Directorate) (NPPD).”[[1]](#footnote-1)

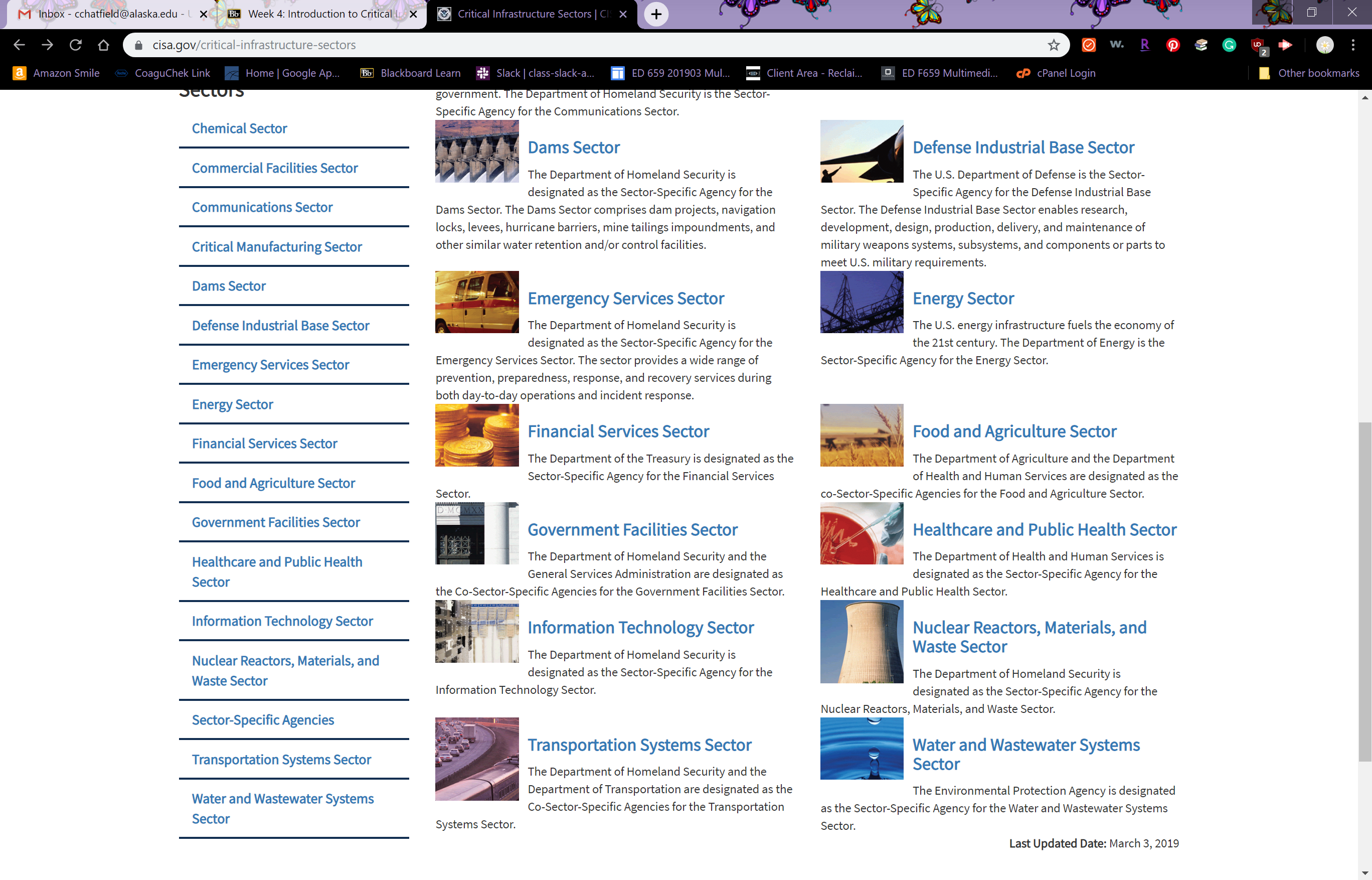
## Identifying Critical Infrastructure

There are currently 16 different critical infrastructure sectors as listed below in this table excerpted from Decision Brief #1.

|  |  |  |
| --- | --- | --- |
| Table 2 – Critical Infrastructure (<https://www.dhs.gov/cisa/critical-infrastructure-sectors>) | | |
| **Identify at least 10 examples for your target city**  **(e.g., examples for at least 10 different critical infrastructures, not 10 examples in one critical infrastructure)** | | |
| **Target City and State:** | | |
| ***Sector*** | ***Example*** | ***Reference*** |
| Chemical |  |  |
| Commercial Facilities |  |  |
| Communications |  |  |
| Critical Manufacturing |  |  |
| Dams |  |  |
| Defense Industrial Base |  |  |
| Emergency Services |  |  |
| Energy |  |  |
| Financial Services |  |  |
| Food and Agriculture |  |  |
| Government Facilities |  |  |
| Healthcare and Public Health |  |  |
| Information Technology |  |  |
| Nuclear Reactors, Materials and Waste |  |  |
| Transportation Systems |  |  |
| Water and Wastewater Systems |  |  |

If you need guidance as to what constitutes critical infrastructure, you can leverage this [website](https://www.cisa.gov/critical-infrastructure-sectors) for additional information





Note that while not specifically called out in this document, CISA has now added information on [UNMANNED AIRCRAFT SYSTEMS (UAS) - CRITICAL INFRASTRUCTURE](https://www.cisa.gov/uas-critical-infrastructure)

In your second Decision Brief Exercise, you’ll be asked to select two targets from Table 2 in Decision Brief #1 and assess their vulnerabilities. You’ll find individual sector plans [here](https://www.cisa.gov/2015-sector-specific-plans)

Why is it important to understand what is critical infrastructure and what is not? Time and resources are always in short supply, so we should be focusing our efforts on those areas that require the greatest amount of response.

You can read more information on CISA [here.](https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html)

Let me know if any of these links change as I would expect this to evolve quickly, given CISA’s recent entry as a new operational component.

## Completing a Vulnerability Analysis

Now that you have identified your target, it’s time to determine how vulnerable it is with respect to physical security, people security and information security. You’ll be asked to evaluate each of these components for your target, to document those assessments on your worksheet and then to link the list of hazards and threats you identified in Decision Brief #1 with the probabilities that you develop in Decision Brief #3 to create your likelihood assessments.

1. <https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency>, accessed November 10, 2019 [↑](#footnote-ref-1)