A key goal of this course is to get you to start thinking about the world in a different way -- to develop what we call the "security mindset". Toward this goal, we will have a small assignment called a "security review" targeted at getting you to think about security on a regular basis, and in contexts where you might not normally think about security.

Submission details. You should submit one security review for this assignment. These security reviews should be short (1-2 pages each). They should be submitted as PDF files, with 12pt fonts, in single-column format with 1-inch margins. You may work individually or in a group of two people. If you work in a group, then the PDF that you upload must include the names of both authors on the first page.

Your goal with the security reviews is to evaluate the potential security and privacy issues with new technologies, evaluate the severity of those issues, and discuss how those technologies could potentially address those security and privacy issues.

The ideal mode of operation is as follows: You might be reading a news source and see the announcement for a new product or service. You immediately start thinking about the security implications and issues associated with the new technology. You then formalize your thoughts (in the framework described below) and submit your writeup to me.

Your security review should contain:

- **Summary of the technology that you're evaluating.** You may choose to evaluate a specific product (like the Miracle Foo) or a class of products with some common goal (like the set of all implantable medical devices). This summary should be at a high level, around one or two paragraphs in length. State the aspects of the technology that are relevant to your observations below. If you need to make assumptions about a product, then it is very important that you state what those assumptions are (i.e., you are evaluating not exactly the Miracle Foo but "something like the Miracle Foo").
- **State at least two stakeholders** (indirect or direct) associated with this technology.
- **State at least two assets and security goals.** Please explain why the security goal is important. This should be around one or two sentences per asset/goal.
- **State at least two potential adversaries and threats.** You should have around one or two sentences per adversary/threat.
- **State at least two potential weaknesses.** Again, justify your answer using one or two sentences per weakness.
- **State potential defenses.** Describe potential defenses that the system could use or might already be using to address your potential weaknesses above.

- **Evaluate the risks** associated with the assets, threats, and potential weaknesses that you describe. Also discuss relevant "bigger picture" issues (ethics, likelihood that the technology will evolve, and so on).
- **Conclusions.** Give some conclusions based on your discussions above. In your conclusions you should reflect thoughtfully on your results above.