COSC 3050, Spring 2016
Whistle Blowing

Case 1:

You are writing a white paper for a new operating system. White papers are a standard way for a business to discuss specifics of a project or projects. Often they are authored by the engineers or designers of the system. It is common to mention strengths and weaknesses in a white paper, but only to a certain degree. Remember that this is a way to provide prospective customers descriptions of your upcoming product.

The operating system you are writing about has a serious security weakness. Is it your duty to insist on revealing this important information in the white paper or through some other means of communication, or even at all?

COSC 3050, Spring 2016
Whistle Blowing

Case 2:

You work at an air traffic control tower and you discover a system vulnerability in one of the software tools used to track planes. This is really big because it potentially endangers many lives. You present the information of this vulnerability to management. The response is that management will pass it on to the appropriate authorities. Two weeks later, you have heard nothing about the vulnerability. You are worried that the problem will soon cause a fatal accident. Your query about the status of your report goes unanswered. Is it ethically acceptable to publicly disclose this information on national television? You know this type of disclosure may instill fear and panic in the public.

(Note: The FAA, FCC, NTSB and other government agencies all work together to provide software and support the hardware for the country's air traffic control systems. The FAA also mandates the certifications for air traffic controllers. Controllers are normally only hired by the FAA. The rest of the support staff is normally hired by the airport facility but must be licensed in their individual area of expertise. And now congress is talking about going to the lowest bidder to manage the National ATC Authority.)

COSC 3050, Spring 2016
Whistle Blowing

Case 3:

You work as a software auditor for a defense firm that is under contract to meet a Department of Defense (DOD) standard. You review the software specification documents for a program, find numerous discrepancies, and write a report about them. When you deliver the report to the Program Manager, he acknowledges receiving the report and then throws it in the shredder bin. Unnerved, you return to your desk and read the DOD standard and learn that his only obligation is to receive the report, not do anything with it. You have put considerable time into preparing this report and believe that following its recommendations would significantly improve the software's quality. Should you confront the Program Manager and request that he read the report, take the issue to management, or do nothing?

COSC 3050, Spring 2016
Whistle Blowing

Case 4:

You find a potentially serious problem in some management and monitoring software that you wrote. Your boss says to ignore it. He says that if there is a problem, the customer will complain soon enough if it affects him or her.

1. Do you take any action?
2. Does is matter what the software is monitoring?
    - Suppose the software is monitoring patients in a hospital?
    - How about monitoring cold-room temperatures in WalMart's Cheyenne distribution hub?
    - What if it is monitoring the flow rates of the individual mix components in a plant making concrete for bridges?

COSC 3050, Spring 2016
Whistle Blowing

Case 5:

You are working on a software project to develop a transportation-related software program for a major metropolitan area. You and your team have worked very hard on this project but discovered some difficulties that could not have been anticipated. That means that the project is behind schedule.

The city transportation planners are nervous because they are depending on your software to get their new transportation system up and running. Your company administration is getting nervous because they signed a contract to deliver the software on time. The contract has significant late penalties. Although the software is not yet foolproof, testing has so far revealed that it works 100% correctly about 99% of the time. The few glitches which remain apply only to the transportation system's backup code, which arguably would only be needed in the most severe of emergencies.

The city planners and the corporate administrators decide to implement the software. The decision is based on the probability of not needing the backup systems for several months, by which time the bugs should be fixed. Both sides also agreed not to announce publicly that the software still as a few bugs. You and your team feel that the bugs are more dangerous than management is willing to admit. What would you do? Defend your position.

COSC 3050, Spring 2016
Whistle Blowing

Case 6:

You are an intern at the Navy's Barking Sands, HI facility. This is a real paradise for a summer job. Your position includes monitoring sensors in various storage areas where weapons systems using Otto II fuel are stored. Otto II fuel can pose a significant health hazard to people and animals.

One of the things you have noticed is that several of the sensors seem to be giving the exact same readings all the time. You have a schedule of the use of the storage areas and some of them that contain the questionable sensors have recently had a significant movement of weapons in and out. But there is not so much as a quiver in any of the readings, even on the sensors designed to detect airborne parts-per-million of Otto II vapors.

You report your findings to the section supervisor with the recommendations that the past history be tracked to see how long the suspect sensors have given the same readings and that the sensors be physically examined or exchanged. The supervisor very brusquely asks you if you like working here or if you want to be sent back to Wyoming before the internship is over? It seems obvious that the supervisor is not going to do anything about the situation. What do you do and why?