Name: _____ **USC ID:** _____

INF 523 Midterm Exam

Fall 2017

Instructions:

Show all work. This exam is open book, open notes. You may use a computer to view materials that you previously stored on your computer, but all communications must be disables (e.e. Airplane mode). This means you can not use the web, D2L, Blackboard, or obtain files from Dropbox or similar services during the exam. You have **120 minutes** to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question**. The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading**.

Be sure to include your **name** and **USC ID** number **on each page**.

There are **100 points** in all and **3 questions.**

	Q1	**Q2**	**Q3**		**Total Score**
Score					

Name: _____ **USC ID:** _____

Election Management Systems – After shocking revelations that other countries may have interfered with the most recent US Presidential election, you have been hired to assess the security of one system being offered to states to manage their elections and tally votes. Fortunately, the system is not providing "internet voting", but rather it manages the lists of authorized voters, ideally only allows authorized voters to cast ballots, correctly tabulates the votes at local "poling" places (these are the physical locations where voters go to cast their votes), transmits those vote tallies to a central location using phone lines or the internet, correctly adds the votes from multiple polling places, and presents the correct result to the designated state official who will certify the results. The desired security policies for the system are that the votes cannot be modified (an accurate tally), that only authorized individuals can cast votes, that all authorized individuals wanting to cast a vote can do so, and that the specific votes of an individual are known only by that individual (secret ballot).

I have intentionally limited the scope of this system to a single state, and you may assume that all polling places in the state will use the same software and election tabulating equipment (this is not an accurate statement of how election are run – many states useful different kinds of equipment in different counties, or even within the same county, but I want you to assume this is a single system for the purposes of these questions).

As discussed in class, you should think like the adversary... You need to consider all kinds of attacks on this "system", not just the obvious ones. What are the implications of each potential line of attack. Consider also that the system must be managed. That means there will be administrators of the various components of the system, each of which may have the ability to compromise the results. When considering your assurance arguments, they must be made under the assumption that some of these administrators might be untrustworthy (this is the insider threat).

Please answer the following questions:

Name: _____ **USC ID:** _____

1. Threat modeling – (50 points)

Given the description of the system, and the parts of the system described earlier,

a) Create a data flow diagram for the system. For simplicity assume there are two polling places where voters use a touchscreen kiosk to cast a vote, two such touchscreen kiosks per polling place, one system managing voter rolls (voter registration – who is allowed to vote), and one system displaying results of the election. (15 points)

b) Describe the adversaries in such a system, in terms of the kinds of access they have to different systems (components of your DFD), and their levels of sophistication. For example, one kind of adversary would be those that can only reach systems through the internet or observe traffic over the internet. (10 points – Answer on Back of Page)

Name: _____ **USC ID:** _____

c) List the potential weaknesses in the system according to the STRIDE model as applied to the DFD created in 1a. (25 points)

Name: _____ **USC ID:** _____

2. Defending the system – List some of the techniques and defensive measure you could apply that will result in improved arguments for assurance in the system. Please include among these techniques those that are 1) architectural – relating to the interrelation of components of the system, 2) software based – relating to the structure of software and the programing of the components, and 3) technological – specific technological techniques or components that can be applied to improve the security and assurance of the system. (35 points)

Name: _____ **USC ID:** _____

3. Assurance After the Fact. In most of our discussion of assurance we were concerned with making arguments that a system is secure and that it will correctly enforce the security policies defined for the system under various operating conditions (i.e security is with respect to a policy and an operating environment). For many systems (especially election systems) we are also interested in retrospective assurance, that the system has correctly enforced the defined policies. In particular we want to be able to make assurance arguments following the election that the voting wasn't rigged. List some techniques or characteristics of the system that will assist in making these retrospective assurance arguments. (15 points)