Reconciled Assessment Tasks from CCI Round 2
November 17, 2014 (draft)

	Topic	Assessment Task
1	security analysis	Given a scenario, identify potential targets and attackers.
2	security analysis	Given a scenario, identify the security goals.
3	security analysis	Given a scenario, devise a security plan.
4	security analysis	Given a scenario, explain why a failure happened.
5	vulnerability	Given a scenario, identify potential vulnerabilities and potential failures.
6	vulnerability	Given a protocol, identify a vulnerability.
7	vulnerability	Given a multi-party protocol, identify vulnerabilities based on people cheating.
8	vulnerability	Given a scenario and change to it, identify new vulnerabilites caused by the change.
9	vulnerability	Given a scenario with faulty functionality or incorrect assumption, identify vulnerabilities caused by that faulty functionality or incorrect assumption.
10	vulnerability	Given a scenario, identify and classify vulnerabilities by categories.
11	vulnerability	Given a scenario, identify vulnerabilites based on gaps between theory and practice.
12	vulnerability	Given a scenario, identify vulnerabilities based on usability issues.
13	risk	Given a scenario, assess the risk of acting and of not acting.
14	risk	Given a scenario, identify risky behaviors.
15	risk	Given a scenario, rank the relative risks of certain possible actions.
16	attack	Given a network scenario, explain how to exploit traffic analysis.
17	attack	Given a policy, devise way to evade it.
18	attack	Given a scenario, assess the difficulty of various attacks.
19	attack	Given a scenario, devise a social engineering attack.
20	attack	Given a scenario, devise an attack that analysts can't identify.
21	attack	Given a scenario, devise an attack.
22	attack	Given a scenario, identify attacks against confidentiality, authentication, integrity, and availability.
23	attack	Given a scenario, identify ways to influence people.
24	attack	Given a system, devise attacks that exploit the role of actors and information outiside of the system.
25	defense	Given a scenario or vulnerability, devise a defense.
26	software	Given a malware example, characterize its behavior.
27	software	Given an example of software, explain how to exploit one of its vulnerabilities.
28	software	Given an example of software, idenitify its vulnerabilities.
29	recovery	Given a breach, explain how to recover from it.
30	out-of-the-box thinking	Solve a puzzle requiring "out-of-the-box" thinking.