#	Question	Your Answer	Your Comments
1	What is the business requirement for this penetration test? 1. This is required by a regulatory audit or standard? 2. Proactive internal decision to determine all weaknesses? For example, is the driver for this to comply with an audit requirement, or are you seeking to proactively evaluate the security in your environment?		
2	What is the business requirement for this penetration test? 1. This is required by a regulatory audit or standard? 2. Proactive internal decision to determine all weaknesses? For example, is the driver for this to comply with an audit requirement, or are you seeking to proactively evaluate the security in your environment?		
3	How many IP addresses and/or applications are included as in scope for this testing In case you need a white box pen test, provide the following: 1. IP address range (Internal & External). 2. Number of total systems/computers/laptops in the network(s). 3. Number of VoIP phones & their make. 4. VPN details for accessing the internal network and carrying out the PT. 5. Few of the staff's email addresses & their names for		

	assessing level of security awareness. *If you need a black box pen test, just provide us with your domain name and nothing else. We will attempt to exploit your network and then give you all identified exposures. After than you review, and then we can attempt the white box pen test. [Tip – black box pentest, helps you know the experts from the crooks! –so we recommend you start with this whoever gives you exploits even before they get to know your network, you go with that one]*		
4	What are the objectives? 1. Map out vulnerabilities 2. Demonstrate that the vulnerabilities exist 3. Test the Incidence Response 4. Actual exploitation of vulnerability in a network, system, or application. 5. Obtain privileged access; exploit buffer overflows, SQL injection attacks, etc. This level of test would carry out the exploitation of a weakness and can impact system availability. 6. All of the above		
5	What is the "target" of the Penetration test? Is it; 1. An Application 2. A Website 3. A Network 4. Application and Network 5. Wireless 6. Other, please explain 7. All of the above – please specify		

6	Do you also want the following tests to be performed? 1. Physical security test – to gain access to physical space by evading physical security controls 2. Social Engineering test – to gain sensitive information from one or more of your employees (to infer or solicit sensitive information) Please explain fully:		
7	What protocol should be followed for alerting on vulnerabilities found? 1. Wait until the end of the testing to report all vulnerabilities 2. Report vulnerabilities as we find them 3. Daily report on the status of the testing 4. Report only critical findings immediately		
8	Will this testing be done on a production environment? You need to understand that certain exploitation of vulnerabilities to determine and/or prove a weakness could crash your system or cause it to reboot. Summit Consulting is not liable for downtime caused by proving the system's weakness to attack.		
9	If production environments must not be affected, does a similar environment (development and/or test systems) exist that can be used to conduct the pen test?		
10	Are the business owners aware of this pen test? Are key stakeholders (business owners) aware that the nature of a pen test is to attack the system as a hacker (or hostile actor) would in		

	order to learn and prove the system's weakness? *In addition to identifying vulnerabilities, if found, we will attempt to exploit them and then show you the results.*		
11	At what time do you want these tests to be performed? 1. During business hours 2. After business hours 3. Weekend hours 4. During system maintenance window 5. Anytime, please explain fully		
12	Who is the technical point of contact, assuming this is not a covert (black box) test of the incident response function? 1. Names: 2. Tel: 3. Mobile: 4. Email:		
13	Provide a dated written consent letter on company headed paper and stamped with the company seal/stamp authorizing for the penetration test to take place and showing duration of test		
14	Additional information?		

And finally, what is your budget?