

2003년도 공공기관 정보보호 수준제고 사업 과제
제안요청서

과제명	특허넷 정보보호 컨설팅 수행 및 정보보호시스템 구축 사업
주관기관명	특허청

2003 년 8 월 일

담당	정보관리담당관실	전산사무관 박성우	TEL:(042)481-5092	FAX:(042)472-3605
	정보관리담당관실	전산주사보 박인화	TEL:(042)481-5164	FAX:(042)472-3605

목 차

1. 추진배경 및 필요성

- 가. 추진 배경
- 나. 사업추진 필요성

2. 제안 목표 및 내용

- 가. 제안 목표
- 나. 내용 및 범위

3. 추진계획

- 가. 추진목표
- 나. 추진방향 및 전략
- 다. 추진체계
- 라. 추진일정 및 내용

4. 소요예산 및 투입인력

- 가. 예산총괄표
- 나. 세부예산 및 투입인력

5. 제안요청내용

- 가. 도입대상 내역 및 구성요건
- 나. 일반요구사항
- 다. 유지보수계획
- 라. 교육지원계획
- 마. 기술지원계획
- 바. 기타

6. 입찰 및 제안서 접수

- 가. 입찰방식
- 나. 제안요건
- 다. 제안서 접수

7. 기대효과

[붙임1] 특허청 정보시스템 및 정보보호시스템 현황

[붙임2] 제안 평가항목 및 배점내역표

1. 추진배경 및 필요성

가. 추진 배경

- 특허청은 특허행정전산화 사업을 수립, 세계 최초로 인터넷기반의 「특허넷 시스템」(’99년)과 「신평급 검색시스템」(’00년)을 성공적으로 개통하여 출원, 심사, 심판, 등록, 공보 발간 등 모든 특허행정이 전산화되어 수행되고 있음
- 특허청이 보유하고 있는 국내외 특허관련 전자문서는 약 15Tbyte로 방대하고, 인터넷을 통해 접수 및 발송되는 대민서비스 자료도 일일 5,000여건에 이르는 등 방대한 자료의 생성과 저장 및 이용이 전산환경에서 처리되고 있으며, 특히 ’03년 7월에는 세계최초로 인터넷기반 전자출원 100만건을 달성하였음
- 21세기 지식정보화 사회의 거의 모든 분야에서 인터넷과 같은 정보기술을 이용하여 시·공간적 우위인 사이버상에서 대량의 정보를 공유하는 업무수행 체제로 급격히 진화하고 있으며 이에 따라 요구되어지는 정보보호의 중요성도 점차 증대되고 있음
- 「1.25 인터넷 대란」, 「7.6 국제해킹대회」 등의 사례와 같이 사이버상에서의 해킹 및 테러가 점차 대규모화, 지능화 되고 있어, 정보 침해사고에 따른 피해도 업무마비 및 업무손실 사태로 심각한 문제를 초래함
- 특허청이 보유한 정보자산은 그 규모가 방대할 뿐만 아니라 특허권 등 국내외 출원인의 지식재산권을 다루고 있어, 정보 침해사고 발생시 업무마비 및 국가 자산의 훼손뿐만 아니라 법적 분쟁의 소지가 있는 중요한 자료이므로 이에 대한 보호가 절실히 필요함

나. 사업추진 필요성

- 최근의 대규모화, 지능화된 보안위협에 대응하기 위한 정보보호체계의 최신 보안수준 유지를 위하여 정형화되고 세분화된 정보보안사고 예방체계 및 대응체계 수립이 필요함
- 최근 증가하고 있는 사이버 테러로부터의 대응책을 마련하여 업무의 연속성을 유지하기 위하여 최신기술을 적용한 모의해킹 및 위험분석을 통해 정보시스템의 실제적인 위험요소의 파악 및 대책수립이 필요함
- 내.외부적 위협요소로부터 항구적으로 시스템을 보호하기 위해 최신의 취약점 분석도구를 도입하여 자체 점검과 대책수립이 필요함
- 특허청 정보자산의 보호와 국내의 정보보호체계 표준을 따르는 정책·지침을 마련하여 특허넷Ⅱ시스템('03 ~ '05년 개발, '06년 개통목표)의 보안기반 구축 필요

2. 제안 목표 및 내용

가. 제안 목표

- 최신기술 및 관리방법을 적용한 체계화된 정보보호정책, 지침, 절차를 수립하여 정보시스템의 보안체계를 강화하고 궁극적으로 대민서비스의 신뢰도 제고
- 최신기술을 적용한 모의 해킹 및 취약점 점검을 통하여 정보시스템의 실제적인 위험요소의 파악 및 대책수립
- 정보시스템의 항구적인 보호를 위해 최신 취약점 분석도구를 도입하여 자체 점검 수행

과제수행기간 : 착수일로부터 2개월

나. 내용 및 범위

○ 정보보호 정책, 지침 및 절차 수립

- 특허청 정보보호의 목적, 대상, 범위, 비전 제시
- 정보보호 조직(청 보안담당 및 위탁업체 보안인원) 구성, 역할, 책임 정의
- 정보보호시스템 운용 및 정보보호업무에 대한 처리지침/절차의 체계화
- 정보시스템 각 분야별(서버, 네트워크, 데이터, PC, 응용, 인증 등) 보호지침
- 신규시스템 개발 등 보안성 평가가 필요한 대상에 대한 보안성 평가절차의 수립
- 청 인원 및 위탁운영업체 보안강화를 위한 관리적, 기술적 보안지침
- 침해사고 즉시 대응 및 복구체계 구축
- 전산당직 및 비상연락체계의 정비
- 특허전산센터 출입통제 등 보호대책 및 전산장비 반출입통제 지침 정비
- 이동식 저장매체 사용 및 문서폐기 관련 지침 정비
- 인원별(보안담당자, 위탁업체, 청 일반인원 등) 보안교육 수행방안
- 효율적인 보안감사 수행방안(수행대상, 수행주기, 수행내용) 등

○ 모의 해킹 및 취약점 점검

- 서버/네트워크 취약점 진단 도구를 이용한 보안취약점 진단 수행
- 진단 도구 및 수동점검에 의한 결과 분석
- 취약점 항목 분석 및 취약점 목록 작성
- 취약점 제거를 위한 보안 대책 수립
- 외부 비인가자에 대한 모의 해킹 테스트
- 내부 비인가자에 대한 모의 해킹 테스트
- 모의해킹에 대한 결과 분석 및 취약점 제거 방안 수립 등

○ 네트워크 취약점 분석도구 도입

- 정기적으로 내부 시스템의 취약점을 점검할 수 있는 네트워크취약점 분석도구 (이동성이 간편한 독립시스템 운영형) 도입, 설치 및 교육

3. 추진 계획

가. 추진목표

○ 최종목표

정보보호 컨설팅을 통해 특허청 정보자산의 보호와 국내외 정보보호체계 표준을 따르는 정책·지침을 마련함으로써 특허청 정보자산을 체계적인 관리모델에 의해 운영하고, 취약점 분석도구의 도입 및 취약점 분석을 통해 다양한 기법으로 취약점을 제거하여 특허청 정보자산을 보호

○ 단계별 추진목표

- 1단계 : 특허청 정보시스템 및 정보자산에 대한 현황 분석, 정보보호정책, 지침, 절차서 작성을 위한 계획 수립 및 취약점 분석도구의 도입, 설치, 운영 방안 수립
- 2단계 : 특허청 정보시스템 및 정보자산에 대한 취약점 분석과 모의해킹 수행 및 정보보호정책, 지침, 절차 수립
- 3단계 : 취약점 분석과 모의해킹 수행결과에 따른 취약점별 대응책 수립 및 정보보호정책, 지침, 절차서의 완성
- 4단계 : 주기적인 정보보호정책, 지침 준수사항 검사 및 주기적 취약점 분석 수행

나. 추진방향 및 전략

○ 추진방향

- 특허청 정보 자산의 보호와 국내외 정보보호체계 표준을 따르는 정책·지침을 마련함으로써 특허넷Ⅱ시스템('03 ~ '05년 개발, '06년 개통목표)의 보안기반 마련
- 특허청 정보 자산에 대한 취약점 분석 및 취약점 제거를 통해 현 시스템의 정보보호를 강화하고, 취약점 분석도구의 도입을 통해 향후 주기적인 자체 취약점 분석 기반 마련

○ 단계별 중점추진사항

단계	중점 추진 사항	비고
1단계	<ul style="list-style-type: none"> . 특허청 정보시스템 및 정보자산에 대한 정확한 현황 분석 . 정보보호정책, 지침 및 절차 수립을 위한 계획 . 취약점 분석도구 도입, 설치 및 운영 방안 수립 	
2단계	<ul style="list-style-type: none"> . 특허청 정보보호를 위한 비전 제시 . 정보보호정책, 지침 및 절차 수립 . 특허청 정보시스템 및 정보자산에 대한 취약점 분석과 모의해킹 수행 	
3단계	<ul style="list-style-type: none"> . 취약점 분석 및 모의해킹 수행결과를 바탕으로 취약점별 대응책 수립 . 취약점 분석 및 모의해킹 수행결과를 정책, 지침에 반영 . 정보보호정책, 지침, 절차서의 완성 및 교육 . 취약점 분석도구 운영 기술 습득 . 컨설팅 제공자로부터 정보보호 관련 기술 습득 	
4단계	<ul style="list-style-type: none"> . 주기적인 정보보호정책 및 지침 준수 현황 검사 . 컨설팅 제공자의 사후 지원을 활용하여 이행 상황 검사 . 정보보호정책 및 지침의 지속적인 갱신 . 주기적 취약점 분석 	

4. 소요예산 및 투입인력

가. 예산 총괄표

(단위 : 원)

구 분	금 액
정보보호컨설팅 용역비	109,518,145
정보보호 시스템 구축비(네트워크기반 취약점 분석 도구)	85,140,000
합 계	194,658,145

나. 세부예산 및 투입인력

1) 정보보호 컨설팅 용역비

(단위 : 원)

구 분	투입 인력	월/단가	M/M	금액	비고
범위선정/환경분석	중급		0.25		
서버진단	중급		0.5		
	초급		0.5		
네트워크진단 (보안장비 진단포함)	중급		0.5		
	초급		0.5		
모의해킹	고급		0.75		
	중급		0.75		
웹어플리케이션진단	중급		1.0		
	초급		1.0		
데이터베이스진단	고급		0.5		
	중급		0.5		
정보보호계획수립	중급		0.25		
정보보안절차 및 지침수립(1)	고급		1.0		
	중급		1.0		
	초급		1.0		
정보보안절차 및 지침수립(2)	고급		1.5		
	중급		1.5		
	초급		1.0		
계				109,518,145	

2) 정보보호시스템 구축비

(단위 : 원)

구분	품명	규격(사양)	수량	금액	산출내역
네트워크기반 취약점 분석도구		Unlimited	1	85,140,000	

5. 제안요청 내용

가. 도입대상 내역 및 구성요건

1) 정보보호 정책, 지침 및 절차 수립

- 국내외 표준을 적용한 정보보호체계 수립
- 특허청 전체 정보시스템, 자산 및 인원에 대한 정보보호 정책, 지침, 절차서 수립
- 정보보호 정책서 요구사항
 - 국내외 일반적인 표준을 준수하고, 특허청 특수사항을 충실히 반영
 - 향후 정보시스템 구성 및 구조 변화를 염두에 둔 유연한 정책제시
 - 특허청 정보보호의 목적, 대상, 범위, 비전 제시
 - 특허청 정보보호 관련 용어 정의
 - 정보보호업무의 체계적인 수행 전략
 - 정보보호 조직 구성, 역할, 책임 정의
 - 정보보호의 대상별(특허전산센터, 서버, 네트워크, 데이터, 응용시스템, 사용자 PC 등) 보호대책
 - 특허전산센터 출입통제 및 재해(화재, 홍수, 연기 등) 대책
 - 청내 및 청외 인가자에 의한 특허청 정보시스템 접근허용 정책 (비인가자로부터의 특허청 정보시스템 접근통제대책)
 - 사용자 및 데이터의 분류를 통한 접근권한관리체계
 - 위탁업체의 특허청 정보시스템 접근에 관한 엄격한 보안관리체계
 - 특허청 정보자산의 보호 및 유연한 특허정보서비스를 위한 망운용 정책
 - 통신로상의 안전한 특허정보의 전송
 - 신규시스템 개발 등 보안성 평가가 필요한 대상에 대한 보안성 평가절차
 - 국내외 외부기관과의 시스템 연계시 준수규정
 - 침해사고 즉시 대응 및 복구체계
 - 전산당직 및 비상연락체계
 - 전산장비 반출입통제 및 이동식 저장매체 사용에 따른 관리대책
 - 체계적인 보안교육 및 보안감사 수행
 - 보안 위규자 처벌규정 등

○ 정보보호 지침/절차서 요구사항

- 정보보호 정책서의 내용을 보다 구체적, 세부적으로 상세히 기술하여야 함
- 지침서와 절차서의 내용 및 기능이 구별되어야 함
- 내용에 대한 타당성 검토와 평가가 수행되어야 함
- 추후 시스템 변경에 따른 개정이 용이하도록 체계적인 개정 방안 수립
- 정보보호의 대상별(특허전산센터, 서버, 네트워크, 데이터, 응용시스템, 사용자 PC 등) 보호지침 및 관련절차 수립
- 특허전산센터 출입통제 및 재해(화재, 홍수, 연기 등) 예방관련 지침 및 절차 수립
- 청내 및 청외 인가자에 의한 특허청 정보시스템 접근허용과 관련한 지침 및 관련절차 수립 (비인가자로부터의 특허청 정보시스템 접근통제지침 및 관련절차)
- 사용자 및 데이터의 분류를 통한 접근권한관리지침 및 관련절차 수립
- 사용자 직무 및 사용자 ID 관리지침 및 관련절차 수립
- 위탁업체의 특허청 정보시스템 접근에 관한 엄격한 보안관리지침 수립
- 특허청 정보자산의 보호 및 유연한 특허정보서비스를 위한 망운용 지침 및 관련절차 수립
- 통신로상의 안전한 특허정보의 전송 지침 및 관련절차 수립
- 신규시스템 개발 등 보안성 평가가 필요한 대상에 대한 보안성 평가지침 및 관련절차 수립
- 침해사고 즉시 대응 및 복구와 관련한 지침 및 절차 수립
- 전산당직 및 비상연락체계와 관련한 지침 및 절차수립
- 전산장비 반출입통제 및 이동식 저장매체 사용에 따른 관리지침 및 절차 수립
- 체계적인 보안교육 및 보안감사 수행지침 및 관련절차 수립
- 외부기관과의 망 연계 관련 표준화된 지침 수립
- 향후 상시 보안관제체계 구축시 운영지침 및 관련절차의 가이드라인 제시
- 기타 관리적, 기술적, 물리적 정보보호와 관련한 지침 및 절차 수립 등

2) 모의 해킹 및 취약점 점검 요구사항

○ 특허청 정보시스템에 대한 사이버 모의해킹을 실시

- 모의해킹 수행 방법 및 툴 명시
- 모의해킹 산출물 및 품질보증 방안
- 기본적인 해킹 기술의 전수 및 교육훈련 방안
- 내부망 침투 방안
- 해킹 결과에 대한 대응 방안 등 기타 필요한 사항

○ 침해사고 발생시 대응능력 강화

- 침해사고 발생시 단계별 구체적인 대응방안 및 모의대응
- 특허청 환경에 적합한 최적의 침해사고대응팀(CERT) 운영 방안
- 침해사고 시나리오별 실전에 의한 대응능력 강화 방안
- 침해사고 분석 기술 및 대응방법 등 기타 필요한 사항

○ 시스템 및 네트워크 취약점 분석

- 특허청 웹서비스용 서버 및 네트워크 등 관련 장비에 대한 취약점 분석
- 취약점 분석 산출물 및 품질보증 방안
- 분석 결과에 따른 대응 방안 등 기타 필요한 사항

3) 네트워크 취약점 분석 도구 요구사항

가) 도입 내역

구분	품명	규격(사양)	수량	인증구분
네트워크기반 취약점 분석도구(S/W)		Unlimited	1	행정정보보호제품

나) 필수요구사항

IP 대역, 호스트 수량에 관계없이(Unlimited) 점검·분석할 수 있는 버전으로 다음 기능을 갖추어야 한다.

기능	세부기능
<p>다양한 네트워크 및 시스템에 대한 정보 수집 및 점검</p>	<ul style="list-style-type: none"> ○ 일반 UNIX, Linux 및 Windows 계열 시스템 ○ Router와 같은 네트워크 장비 ○ Firewall, IDS와 같은 보안장비 ○ 점검 대상 호스트의 운영체제에 비종속적 ○ OS 자동탐지 및 정밀 Portscan 기능 제공 ○ 점검 모듈간 결과를 상호연동하기 위한 Data Repository 운영 ○ 다양한 종류의 데이터베이스 취약점 점검 ○ 발견된 취약점에 대해 취약점의 특성에 따라 위험도 등급을 분류
<p>다양한 서비스 정보 수집</p>	<ul style="list-style-type: none"> ○ 점검 대상의 열려있는 포트 점검 ○ 열린 포트들에 Binding된 각종 네트워크 서비스들이 제공하는 옵션과 Banner 정보, 버전 정보 등의 정보 수집(Web Server, FTP, Telnet 등) ○ 다양한 사용자 옵션 제공(점검할 네트워크 서비스의 선택기능 등 옵션제공) ○ SQL injection 취약점 점검
<p>다양한 취약점 데이터베이스 제공</p>	<ul style="list-style-type: none"> ○ 취약점 설명(해당 OS, 서비스 종류, 사용 포트번호, 위험도 등의 상세 설명 자료) ○ 조치방법 설명(취약점을 해결하기 위한 설명 자료 및 관련 Site Link)

기능	세부기능
다양한 리포팅 기능	<ul style="list-style-type: none"> ○ 취약점 점검 결과를 네트워크의 보안성을 높이기 위한 기초 자료로서 활용할 수 있는 다양한 형식의 리포트와 취약점의 변동 과정을 알 수 있는 취약점 추세 리포트 제공 ○ 8가지 형태의 리포트에 6가지 형태의 저장방식 지원 ○ 전문 리포팅툴인 크리스탈 리포트를 이용한 리포트 작성 ○ 기간별 취약점 분석 추이 분석 ○ 한글 결과보고서 제공 기능
점검 모듈의 수동.자동 업데이트 기능	<ul style="list-style-type: none"> ○ 수동 업데이트(사용자가 인터넷을 이용하여 패치를 내려받아 직접 설치하는 방법) ○ 자동 업데이트(사용자의 조작없이 전용 Update 프로그램을 이용하여 새로운 점검 모듈을 자동으로 내려받아 설치하는 방법) ○ Scan 항목이 자동으로 업데이트
설치가 용이하고 사용이 간편	<ul style="list-style-type: none"> ○ 설치프로그램 제공으로 간편하게 설치를 수행할 수 있어야 함 ○ 설치 후 리부팅과 같은 별도의 조작없이 One Click으로 진단 수행 가능 ○ 점검 내역이 실시간으로 리포팅 되어야 함
작업내역이 세션으로 관리 가능	<ul style="list-style-type: none"> ○ 작업단위 구성 및 재사용(세션단위 Open, Save, Load 가능) ○ 세션별 점검내역 관리 기능 제공(History 관리 기능) ○ 취약점 점검, 리포팅 등의 작업에 세션별 관리
스케줄링 작업이 가능	<ul style="list-style-type: none"> ○ 스케줄링에 의한 점검 작업 및 리포팅의 자동화 ○ GUI의 예약 메뉴에서 스케줄링 ○ Email 주소 지정시 작업결과가 압축되어 메일로 배달 가능
기타	<ul style="list-style-type: none"> ○ Multi-Thread로 한꺼번에 여러 시스템에 대한 병렬 점검이 가능해야 함 (사용자의 시스템 자원이 허용하는 한도내에서 최대 100대의 시스템을 동시에 점검 가능) ○ 타 보안제품과의 통합 여부

나. 일반요구사항

- 제안사는 사업의 성공적 추진을 위하여 신의, 성실의 의무를 진다.
- 제안사는 계약 후 2개월 이내에 특허청 정보보호 컨설팅 및 정보보호시스템 구축사업을 완료하여야 한다.
- 과업 수행 및 과업수행 결과물은 정보통신기반보호법, 관련 지침 및 기준과 전산망보안관리규정 등의 관련 법규를 따라야 한다.
- 과업수행과 관련한 안전사고와 기존 장비 및 시설에 대한 피해는 제안사가 배상의 책임을 진다.
- 계약서에 대하여 제안사와 주관기관간의 해석상의 이견이 있을 경우에는 주관기관의 해석에 따라야 하며, 또한 특별히 명시되지 않은 사항은 일반 계약기준을 따른다.
- 전산망보안관리규정에서 정하는 바에 따라 제안사는 과업에 참여하는 인원에 대한 사전 보안승인을 받아야 한다.
- 제안사는 과업수행 과정에서 습득하는 모든 자료 및 정보와 산출물에 대한 보안관리방안을 상세히 제시하여야 한다.
- 제안사는 과업수행 중 발생하는 각종 산출물(보고서 포함)의 명세서와 필수 구성내역 등을 상세히 제시하여야 한다.
- 제안사는 원활한 과업수행을 위한 품질보증 등 과업관리방안을 제시하여야 한다.
- 제안사는 본 제안요청서에서 언급하지 않았으나, 본 과업수행 및 보안성 향상에 도움이 되는 사항이 있을 경우 이를 추가로 제시할 수 있다.

다. 유지보수계획

- 제안사는 본 과업과 관련하여 다음 사항에 대하여 상세히 제안하여야 한다.
 - 무상 유지보수 기간
 - 유지보수의 범위, 지원조직 및 인원, 지원방안
 - 공급한 제품에 대한 Version Upgrade 계획(정책)
 - 시스템 운영 초기 장애대비 및 예방점검 방안
 - 장애 예방대책, 장애발생시 지원방안 및 신속한 복구방안

- 제안사는 무상 유지보수 기간의 종료 후에도 주관기관의 요청에 따라 유상 유지보수 계약을 별도의 조건으로 체결할 수 있으며 조건은 정부 구매 기준에 따른다. 이때 유상 유지보수 활동 내역은 구체적으로 명시하여야 한다.
- 제안사는 시스템 유지보수 및 문제발생시 신속한 해결을 위해 지원체계와 유지보수 절차를 제시하여야 한다.
- 제안사는 협력업체의 도산 및 폐업으로 인해 지원체계에 문제가 발생할 수 있으므로 이의 대처방안을 제시하여야 한다.

라. 교육지원계획

- 교육 대상을 구분하여 교육내용, 기간, 방법 등을 명시하여 상세하게 제시
- 필요한 매뉴얼 목록 및 제공 부수 명시

마. 기술지원계획

- 기술지원 방법, 기술지원 인력 및 조직, 기술 제공 및 이전 방안 제시
- 향후 기술발전 방향 및 신제품 출시에 대한 대책 제시
- 시스템 운영요원의 자체 유지보수 능력 지원

바. 기타

1) 제안서 작성시 유의사항

- 제안서는 「5.바.2) 제안서 목차」에 명시된 형식에 따라 작성하여야 하며, 필요한 경우 주어진 목차 이외의 사항을 추가할 수 있다.
- 본 제안요청 범위를 포함하여 구체적으로 작성하여야 한다.
- 제안서는 용어 설명을 덧붙인다.
- 제안서의 내용은 명확한 용어를 사용해서 표현해야 하며, "~을 제공할 수 있다." "~이 가능하다." 등의 모호한 표현은 평가시 "할 수 없다"로 간주한다.
- 제안서 분량은 A4용지 200쪽 내외로 작성한다.
- 제안요약본 분량은 A4용지 30쪽 내외로 작성한다.

- 제출된 제안서의 모든 내용은 주관기관의 요청이 없는 한 추가되거나 삭제될 수 없다.
- 주관기관은 제안 내용에 대한 확인을 위하여 추가자료 요청 또는 현지 실사를 할 수 있으며, 제안사는 이에 응하여야 한다.
- 제안요청서의 모든 조건은 제안서에서 명백하게 배제된 경우를 제외하고는 묵시적으로 승인되어 제안서에 포함된 것으로 간주한다.
- 제출된 제안서는 일체 반환하지 않으며, 제안서 작성 등에 소요된 제반 비용은 제안사의 부담으로 한다.
- 제안사가 제출한 제안서는 주관기관의 소유로 한다.
- 본 제안요청서의 전체 또는 일부는 제안서 제출 외의 어떤 목적으로도 사용되어서는 안되며, 제안사는 본 사업과 관련하여 취득한 모든 정보를 유출 또는 누설하여서는 안 된다. 이와 관련하여 발생하는 모든 민·형사 상의 책임은 제안사에게 있다.
- 제출된 제안서의 내용 중 허위 기재사항이 발견될 경우 그 중요도에 따라 계약의 무효 또는 부적당업체로 제안사를 제한할 수도 있으며, 차후 정부 및 공공기관에서 발주하는 입찰 참여를 제한 받을 수도 있다.

2) 제안서 목차

제안서의 목차는 다음과 같은 형태(서식)를 반드시 준수하여야 하며, 필요에 따라 소항목을 추가할 수 있다.

1. 제안 개요
 - 1.1 제안 목적
 - 1.2 수행 범위
 - 1.3 추진방향 및 주요내용
 - 1.4 기대 효과
 - 1.5 제안의 특징 및 장점

2. 특허넷 정보보호 컨설팅 수행 및 정보보호시스템 구축 방안

2.1 정보보호정책, 지침, 절차의 수립

- 2.1.1 정보보호정책, 지침, 절차의 수립 전략
- 2.1.2 정보보호정책, 지침, 절차의 수립 방법론
- 2.1.3 정보보호정책, 지침, 절차 수립의 대상 및 범위
- 2.1.4 단계별 세부 추진계획
- 2.1.5 단계별 산출물
- 2.1.6 컨설팅 수행이후 정보보호정책, 지침, 절차의 관리방안
- 2.1.7 기대 효과

2.2 모의 해킹 및 취약점 점검

- 2.2.1 모의 해킹 및 취약점 점검 수행 전략
- 2.2.2 모의 해킹 및 취약점 점검 수행 방법론
- 2.2.3 모의 해킹 및 취약점 점검 수행의 대상 및 범위
- 2.2.4 단계별 세부 추진계획
- 2.2.5 단계별 산출물
- 2.2.6 모의 해킹 및 취약점 점검 수행 결과에 따른 대책수립 방안
- 2.2.7 컨설팅 수행이후 모의 해킹 및 취약점 점검의 주기적 수행방안
- 2.2.8 기대 효과

2.3 네트워크 취약점 분석 도구의 도입

- 2.3.1 네트워크 취약점 분석 도구 선정 기준 및 배경
- 2.3.2 네트워크 취약점 분석 도구의 상세사양, 기능, 성능, 장점
- 2.3.3 네트워크 취약점 분석 도구 도입, 설치 및 시험운영 계획
- 2.3.4 네트워크 취약점 분석 도구 도구를 이용한 효과적 수행방안
- 2.3.5 기대 효과

3. 사업관리부문

- 3.1 품질보증계획
- 3.2 추진일정계획
- 3.3 보고 및 검토계획
- 3.4 수행조직 및 업무분장
- 3.5 투입인력 및 이력사항
- 3.6 인원관리 및 보안대책

4. 지원부문

- 4.1 유지보수계획
- 4.2 교육지원계획
- 4.3 기술지원계획
- 4.4 기타 지원사항

5. 제안 업체 소개

- 5.1 일반현황
- 5.2 조직 및 인원
- 5.3 주요 사업 내용
- 5.4 유사 사업 참여경험 및 실적
- 5.5 관련분야 보유기술

3) 계약체결 및 과제수행상의 유의사항

- 주관기관은 이 제안요청 등에 포함되어 제공된 정보에 정확성을 기하기 위하여 최선을 다할 것이나 각 제안사가 가능한 한 제시된 정보들의 정확성에 대해 스스로 확인할 것을 권고한다. 주관기관과 전담기관은 제안요청서나 기타 첨부자료상의 오류나 누락에 대하여 책임을 지지 않는다.
- 본 제안에 의해 사업자로 선정된 제안사에 대한 주관기관의 통보와 후속되는 계약서 작성이 완료될 때에 비로소 본 계약이 체결된 것이며, 계약체결 전까지 발생한 어떠한 서비스와 관련해서도 제안사는 일체의 법적 우선권을 주장할 수 없다.
- 과제수행자는 계약일로부터 10일 이내에 과제수행계획서와 기타 과제수행에 필요한 제반서류를 제출하고, 과제수행중 내용변경이 불가피할 경우에는 주관기관과 사전 협의하여 변경할 수 있다.
- 주별, 월별 진도보고서를 작성 제출하여 진도 확인을 받아야 한다.
- 과제수행 완료시 과제완료보고서를 작성 제출하여야 한다.
- 본 과제에 참여하는 자는 정보보호컨설팅 및 CERT서비스에 대한 충분한 기술과 경험 등을 가진 자이어야 하며, 과제를 수행함에 있어 주관기관이 부적당하다고 판단하거나 태만하다고 인정되는 종사자에 대해서는 교체를 요구할 수 있으며, 이때 과제수행자는 해당종사자를 즉시 교체하여야 한다.
- 과제수행자는 과제 수행에 참여한 종사자를 임의로 교체할 수 없으며, 불가피한 사유가 발생하였을 경우에는 주관기관과 협의하여야 한다.
- 과제수행자는 사업수행에 따라 생산되는 산출물 및 기록에 대하여는 주관기관의 승인없이 타인에게 제공, 대여, 열람 등을 할 수 없으며, 이에 대한 보안방안을 상세히 제시하여야 한다.
- 본 과제를 수행함에 있어 필요한 경우 분야별 외부전문가를 추가로 투입할 수 있으며, 추가 투입시 주관기관의 승인을 얻어야 한다.
- 주관기관은 과제수행 중 제안서의 내용이 사업의 목적에 미흡하다고 판단되면, 과제수행자와 협의에 의해 사업내용을 추가 또는 변경을 수행할 수 있다.
- 과제수행자는 본 사업의 원활한 수행을 위하여 주관기관과 협의하여 주관기관의 관련자를 포함하는 전담반 및 자문단을 구성·운영하여야 한다.

6. 입찰 및 제안서 접수

가. 입찰방식

1) 사업자 선정 방식

- 소프트웨어사업의협상에의한계약체결기준 (정보통신부 고시 제2000-84호)에 따른 사업자 선정
 - 기술평가 결과 평가점수가 만점의 80%(80점/100점) 이상인 업체를 협상 대상후보자로 선정
 - 협상대상후보자의 기술평가점수(90%)와 가격평가점수(10%)를 합한 점수의 고득점 순으로 협상대상자 선정
 - 협상대상자 중 가장 점수가 높은 자를 우선협상 대상자로 선정하여 협상에 의해 낙찰자 선정
- ※ 제안서 평가 결과 최고점수를 얻은 제안자가 2인 이상인 경우 기술평가점수의 순서에 따라 우선협상 대상자를 정하고 기술평가점수가 동일한 경우에는 기술평가의 배점이 큰 평가항목에서 높은 점수를 얻은 자로 한다.

2) 기술평가 방법

- 기술평가 기준 및 배점은 『제안 평가항목 및 배점내역표』에 의하며(붙임2 참조), 제안서에 기술되지 않은 사항은 0점 처리한다.
- 세부적 평가기준 및 평가결과는 공개하지 않으며, 제안업체는 평가결과에 대하여 이의를 제기할 수 없다.
- 평가위원들의 평가점수를 평균하여 평가점수 산정
 - 평균점수는 소숫점 이하 한자리까지 계산하되 내림 적용
예) 평균점수 79.99은 79.9점으로 계산

나. 제안요건

- 소프트웨어산업진흥법 제24조 및 정보통신부 고시 제1996-56호의 소프트웨어 사업자 신고요령에 의한 소프트웨어 사업자로 등록된 자
- 정보보호컨설팅 서비스 공급업체는 정보통신기반보호법 제17조 규정에 의해 지정된 정보보호컨설팅전문업체로 제한
- 정보보호시스템은 국정원으로부터 인증 받은 제품 또는 전자정부법 제25조 규정에 의해 지정된 행정정보보호용 시스템 제품으로 제한

다. 제안서 접수

- 제안서는 대표자 인감을 날인하여 공문으로 제출하여야 한다.
- 제안서 및 관련 서류는 제출기한 내에 정해진 장소에 직접 제출하여야 하며, 우편접수 및 기타 통신수단에 의한 접수는 불가하다.
- 제출서류
 - 제안서 및 요약서 각 10부 및 파일을 담은 CD 5장
 - 제안서에 기재된 사실을 증명할 수 있는 입증서류
 - 별도 밀봉한 가격 제안서(제품별, 투입인력별 상세 제시)
- 제안서 제출 마감일 : 9월 5일(금) 17:00
- 제안서 제출장소 : 대전시 서구 둔산동 920번지 정부대전청사 4동 1402호
특허청 총무과(용도계)

7. 기대효과

- 특허청 정보시스템 및 정보자산에 대한 보안성 및 신뢰도 제고
 - 전문 컨설팅업체에 의한 최신기술 및 관리방법을 적용한 체계화된 정보보호정책, 지침, 절차를 수립하고, 취약점 점검과 모의해킹의 수행 및 대책수립을 통해 청내·외부로부터의 보안위협에 대한 사전 방어를 강화하여 특허청 정보시스템 및 정보자산에 대한 보안성과 신뢰도 제고

- 특허청 정보시스템 및 정보자산의 체계적인 관리 강화
 - 전문 컨설팅업체에 의한 최신기술 및 관리방법을 적용한 체계화된 정보보호정책, 지침, 절차의 수립과 취약점 점검도구를 통한 주기적인 취약점 점검 및 분석을 통해 특허청 정보시스템 및 정보자산에 대한 체계적인 관리강화의 기틀 마련

- 특허넷Ⅱ시스템 개발의 보안기반 마련
 - 체계화된 정보보호정책의 수립과 정보보호를 위한 관리적, 기술적 비전의 제시는 특허청 정보보호의 중장기 계획수립과 특허넷Ⅱ시스템 개발의 보안기반 마련

- 최신기술 및 관리방법론 획득
 - 정보보호정책, 지침, 절차 수립과 취약점 점검, 모의 해킹 및 대책 수립에 관련한 최신기술 및 관리방법론을 전문가로부터 교육받을 수 있는 기회 획득

[붙임 1] 특허청 정보시스템 및 정보보호시스템 현황

1. 정보시스템 현황

가. 서버

구 분	수 량	용 도
UNIX 서버	32	특허업무처리, 검색, 포탈, 홈페이지, KMS, 망관리, 통합관리 등
NT 서버	17	대민서비스, 콜센터 등
기타서버	5	전자결재 등
SUN	5	보안관련 서버 등
서버 총합	59	

나. 저장 장치

구 분	수 량	용 도
디스크	23	특허업무 데이터 저장, SAN Switch 등
백업장비	5	데이터 백업
JUKE BOX	20	검색 데이터 저장
저장장치 총합	48	

다. 네트워크 장비

구 분	수 량	용 도
네트워크 장비	260	라우터 등 시스템 통신장비
네트워크장비 총합	260	

2. 정보보호시스템 현황

분 야	정보보호시스템
네트워크 보안	침입차단 시스템
	침입탐지 시스템
	가상 사설망
시스템 보안	호스트기반 침입탐지
	사용자 권한관리
	서버취약점 분석도구
	바이러스 백신프로그램
응용시스템 보안	청내 통합인증 PKI
	전자출원 PKI
물리적 보안	폐쇄회로 시스템(CCTV)
	지문인식 시스템

[붙임 2] 제안 평가항목 및 배점내역표

대항목	중항목	세부평가항목	배점	비고
과제수행 부문			55	
	대상업무의 이해도	<ul style="list-style-type: none"> ○ 문제과약의 정확성 ○ 업무이해의 완전성 ○ 제안요청서와 일치성 	(10)	
	컨설팅 수행 전략 및 방법론	<ul style="list-style-type: none"> ○ 정보보호정책, 지침, 절차 수립전략 및 수행방법론의 적정성 및 타당성 ○ 모의해킹 및 취약점 분석 수행전략 및 수행방법론의 적정성 및 타당성 ○ 단계별 추진계획 및 산출물의 적정성 ○ 추진일정 및 투입인력의 적정성 ○ 향후 추가적용의 유연성 ○ 사후 관리 및 지원 대책 ○ 교육지원 및 기술지원계획 	(35)	
	네트워크 취약점 분석도구의 적정성	<ul style="list-style-type: none"> ○ 네트워크 취약점 분석 도구 선정의 타당성 ○ 기능 및 성능의 적정성 ○ 도입, 설치 및 시험운영 계획 ○ 교육지원 및 유지보수 계획 ○ 효과적 취약점 분석 수행방안 	(10)	
사업관리 부문			15	
	관리방법론	<ul style="list-style-type: none"> ○ 문서화 계획 및 보고 계획 ○ 일정관리 및 위험관리 ○ 인원관리 및 보안 ○ 수행조직 및 업무분장 ○ 투입인력 및 이력사항 	(10)	
	품질보증방안	<ul style="list-style-type: none"> ○ 품질보증계획 ○ 품질보증기준 준수 ○ 국제/국내 품질인증 획득 	(5)	

대항목	중항목	세부평가항목	배점	비고
제안사 일반사항			15	
	사업수행능력	<ul style="list-style-type: none"> ○ 대외인지도 및 신용도 ○ 재무구조 ○ 전문진단인력 및 사업수행조직 	(5)	
	방법론과 보유기술	<ul style="list-style-type: none"> ○ 자체 컨설팅 방법론 및 관련기술의 보유 여부 ○ 유사 사업실적 	(10)	
지원부문			15	
	유지보수 계획	<ul style="list-style-type: none"> ○ 유지보수 전략 ○ 유지보수 지원체계 및 절차 ○ 유지보수 조직 및 인력지원 방안 ○ 기술발전에 대한 고려 ○ 장애복구 및 예방점검 방안 	(10)	
	교육 및 기술지원	<ul style="list-style-type: none"> ○ 교육훈련의 조직, 내용, 방법, 일정 ○ 사용자 지침서 제공계획 ○ 관련기술 지원계획 	(5)	