Temat nr 32.		
lp.	**Nazwa programu/projektu**	**cybercrypt@gov - rozproszony, skalowalny, wysokowydajny system pozwalający na przełamywanie zabezpieczeń kryptograficznych**
1	**Zgłaszający**	Komenda Główna Policji
2	**Określenie obszarów obronności i bezpieczeństwa państwa**	Przedmiotem projektu będzie pozyskanie i rozwój technologii niezbędnej do stworzenia rozproszonego, skalowalnego, wysokowydajnego systemu służącego przełamywaniu zabezpieczeń kryptograficznych. Rozwiązanie wpisuje się w priorytetowy obszar technologiczny pn. "*Technika kryminalistyczna*, *nowoczesne technologie lub rozwiązania innowacyjne w sferze bezpieczeństwa teleinformatycznego, ochrony informacji w systemach i sieciach teleinformatycznych oraz narodowej kryptografii".* Został on *,* określony dla 7. strategicznego kierunku badań naukowych i prac rozwojowych "*Bezpieczeństwo i obronność państwa*", ustalonego w Krajowym Programie Badań (KPB). Wdrożenie wyników projektu ma służyć pozyskaniu priorytetowej zdolności operacyjnej służb odpowiedzialnych za bezpieczeństwo, do wspomagania procesu wykrywczego i zwalczania przestępczości (w tym zorganizowanej oraz przeciwdziałania terroryzmowi), o której mowa w KPB. Cyberbezpieczeństwo to jeden z podstawowych obszarów działań Unii Europejskiej na lata 2016-2020, rozwijany i wspierany przez Narodowe Centrum Badań i Rozwoju, Ministerstwo Spraw Wewnętrznych, Ministerstwo Cyfryzacji, Prokuraturę Generalną i Komendę Główną Policji Rzeczypospolitej Polskiej. Dzieje się tak ponieważ znacząco wzrosło zagrożenie cyberterroryzmem oraz cyberatakami ze strony świata przestępczego czy państw trzecich. Na całym świecie istnieją profesjonalne organizacje przestępcze, których celem jest łamanie zabezpieczeń systemów komputerowych, urządzeń Internet of Things i e-health, szyfrowanie danych w celu uzyskania okupu (ransomware) oraz ich ukrycia przed organami ścigania, jeśli zawierają treści przestępcze, w tym komunikację między przestępcami.
3	**Opis projektu**	W ostatnich latach notuje się niepokojący, niezwykle dynamiczny wzrost przestępstw z użyciem nowoczesnych technologii, utrudniający, często wręcz uniemożliwiający wykrycie przestępstwa. Należy zwrócić szczególną uwagę na zagadnienie szyfrowania danych, coraz częściej stosowanych przez przestępców. Niepokoi coraz szersza dostępność i skuteczność dostępnych bezpłatnie algorytmów szyfrujących. Obecnie dane mogą być przesyłane w niezauważony sposób w ułamku sekundy na drugi koniec świata lecz także bez obawy na ich wykrycie składowane na nośnikach i fizycznie przewożone. W wielu przypadkach nie będzie nawet możliwe wykrycie plików przestępczych. W codziennej praktyce badań informatycznych laboratoriów kryminalistycznych w Polsce (nie tylko policyjnych) coraz częściej ma się do czynienia z zaszyfrowanymi i zabezpieczonymi nośnikami danych, w tym urządzeń mobilnych takich jak telefony komórkowe. Moc obliczeniowa zwykłych stacji roboczych, w które wyposażone są służby jest często niewystarczająca aby dokonać przełamania zabezpieczeń średniego poziomu, nie mówiąc o zabezpieczeniach najbardziej wyrafinowanych. Podstawowym celem projektu jest zwiększenie możliwości wykrywczych organów ścigania, wyposażając je w możliwości techniczne adekwatne dla zagrożenia, co usprawni ściganie cyberprzestępstw, zorganizowanej przestępczości oraz cyberterroryzmu.

		Koniecznym jest opracowanie specjalizowanego, wydajnego, rozproszonego, skalowalnego i zdecentralizowanego rozwiązania. Wydajność projektowanego systemu powinna zostać zapewniona poprzez opracowanie wydajnych algorytmów dekodujących, zwłaszcza algorytmów optymalnie dzielących zadania między urządzeniami dostępnymi w istniejącej bazie sprzętowej na której system będzie uruchomiony. System opierać powinien się o wydzielone jednostki zarządzające, w uproszczeniu nazwane serwerowymi, kierujące procesem przetwarzania danych i przydziału zadań. Decentralizacja zarządzania powinna zostać zapewniona przez redundancję zadań wykonywanych nie w jednym centralnym serwerze, a kilku umieszczonych w różnych lokalizacjach, mogących przejmować kontrolę w przypadku uszkodzenia, wyłączenia nawet na skutek ataku. Kolejnym krokiem powinno być połączenie w sieć obliczeniową komputerów ogólnego zastosowania, spoza wydzielonych, objętych tajemnicą służbową komputerów. Skalowalność oznacza, że w każdym momencie, można dołączyć lub odłączyć, z zachowaniem odpowiednich procedur, dowolną liczbę komputerów bez zachwiania integralności prowadzonych obliczeń. Wydajność obliczeniowa może być w ciągły sposób podnoszona przez dołączanie kolejnych komputerów. Najważniejszą cechą tak zdefiniowanego systemu jest "naturalny" proces zwiększania mocy obliczeniowej. Odbywa się on podczas każdej kolejnej wymiany zamortyzowanego sprzętu, co stanowi najważniejszą zaletę w stosunku do systemów opartych o pracę specjalistycznego dedykowanego sprzętu, który starzeje się bardzo szybko wymagając niezwykle kosztownej wymiany. Utworzone oprogramowanie nie powinno gromadzić danych / przetwarzać ich / skanować zawartości komputerów, na których będzie uruchomione. Jedyną funkcjonalnością projektowanej aplikacji powinno być wykonywanie matematycznych kalkulacji kryptograficznych na dostarczonych przez aplikację serwera, niewielkich porcjach danych. Stąd też aplikacja nie powinna zostać wyposażona w mechanizmy pozwalające na ingerencję bądź pobieranie danych z uruchomionych systemów. Dodatkowo, opracowana aplikacja, wytworzone systemy powinny przejść dodatkowy audyt programistyczny. Przewiduje się, że projektowany system powinien pozwalać na przełamywanie haseł opartych m.in. o MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-3 (Keccak), NetNTLMv1, NetNTLMv1+ESS, NetNTLMv2, sha256crypt, sha512crypt a także próbę przełamania zabezpieczeń programów m.in, office 2007,2010,2013, PDF, KeePass, 7-zip, Rar oraz powszechnie stosowanych aplikacji szyfrujących (truecrypt,veracrypt, bitlocker). Podsumowując w ramach niniejszego projektu wykonane zostać powinno zdecentralizowane i skalowalne narzędzie, o bardzo wysokiej efektywności wykorzystania posiadanej mocy obliczeniowej, pozwalające na podjęcie skutecznych prób odszyfrowania danych przy użyciu mocy obliczeniowej aplikacji klienckich, które powinno być przystosowane do działania w oparciu o już istniejącą infrastrukturę informatyczną Policji. Zrealizowany system powinien zostać oparty o rozproszoną architekturę, wykorzystującą moc obliczeniową komputerów, w tym wyposażonych w procesory oraz jednostki GPU, z użyciem zaawansowanych algorytmów obliczeń rozproszonych i równoległych, w której rolą centralnego serwera (o rozproszonej redundantnie funkcjonalności sprzętowej) oraz utworzonego na potrzeby projektu oprogramowania będzie jedynie „koordynowanie” pracy komputerów klienckich, poprzez: • zarządzanie bazą danych zadań i dostępnych zasobów, • kolejkowanie zaplanowanych zadań (rola serwera harmonogramów/scheduler), • przesyłanie jednostkom klienckim stosunkowo niewielkich porcji danych, • odbieranie od nich wyników przeprowadzonych obliczeń oraz

		• testowanie uzyskanych wyników złamanych haseł i podejmowanie decyzji o zakończeniu lub kontynuowaniu pracy. Centralny serwer nie powinien być wykorzystywany do prowadzenia czasochłonnych obliczeń. Utworzone w ramach projektu aplikacje klienckie miałyby na celu analizę aktualnego obciążenia komputera i inicjowanie obliczeń związanych z przełamywaniem zabezpieczeń jedynie w momencie niewielkiego obciążenia sprzętu komputerowego oraz automatyczne przerywanie pracy w przypadku wykrycia zwiększonego zapotrzebowania na moc obliczeniową przez użytkownika. Działanie aplikacji klienckiej i wykonywanie obliczeń powinno odbywać się w sposób niezauważalny dla użytkownika komputera. Aplikacje wytworzone w ramach projektu nie mogą przetwarzać danych które stanowią materiał dowodowy z prowadzonych postępowań procesowych. Jedyną przetwarzaną informacją powinny być kryptograficzne jednokierunkowe funkcje skrótu (a więc dane nie stanowiące materiału dowodowego i nie zawierające materiałów prawnie chronionych). Warto przy tym podkreślić, że w chwili obecnej, zgodnie z obowiązującymi przepisami prawa, prowadzone są działania i czynności, które mają doprowadzić do odszyfrowania danych, jednak z uwagi na niewystarczające moce obliczeniowe oraz technologiczne, działania takie są mało skuteczne. Ponadto co warte podkreślenia, stworzony system powinien pozwalać na przesyłanie do analizy i łamania jedynie danych związanych z czynnościami procesowymi, wyłącznie na wniosek organów ścigania (tj. policji, prokuratur, sądów) a prowadzonych na potrzeby przygotowywanych opinii bądź ekspertyz.
4	**Określenie celu głównego i celów szczegółowych oraz ich relacji do celów innych programów i projektów, a także wskazanie planowanych do uzyskania poziomów gotowości technologii, o których mowa w załączniku do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie sposobu zarządzania przez**	Głównym celem projektu jest opracowanie technologii i przetestowanie narzędzia w warunkach zbliżonych do rzeczywistych pozwalającej organom ścigania na prowadzenie skutecznych ataków siłowo-słownikowych na zabezpieczone zasoby cyfrowe, zabezpieczone podczas postępowania dowodowego, zaszyfrowanych w celu ukrycia treści prawnie zabronionych, komunikacji między przestępcami itp., do których w chwili obecnej nie ma możliwości uzyskania dostępu. W związku z tym podstawowym rezultatem realizacji projektu będzie podniesienie skuteczności w odczytywaniu zaszyfrowanych danych, zarówno w trakcie prowadzonych postępowań operacyjnych jak i trwających postępowań karnych. Celami szczegółowymi projektu będzie: - opracowanie wydajnych algorytmów przetwarzania rozproszonego, - opracowanie metod wydajnego przetwarzania danych przy użyciu procesora oraz kart graficznych, - opracowanie prototypu aplikacji serwerowej, - opracowanie prototypu aplikacji klienckiej, - opracowanie prototypu aplikacji służącej pozyskiwaniu danych z plików, - zaprojektowanie całościowej struktury systemu informatycznego. Założenia projektu są zgodne z następującymi priorytetami strategii krajowych: • ***Priorytety i zadania priorytetowe Komendanta Głównego Policji na lata 2016-2018***, a w szczególności**:**

	Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa, w tym dla technologii krytycznych o znaczeniu determinującym powodzenie całego programu lub projektu	➢ Priorytet 2.: Podniesienie skuteczności działań Policji w identyfikacji i zwalczaniu największych współczesnych zagrożeń, w tym cyberprzestępczości: zadania 3, 7, 8; ➢ Priorytet 6.: Podniesienie jakości i efektywności pracy Policji poprzez sukcesywne podwyższanie kompetencji zawodowych funkcjonariuszy i pracowników Policji: zadania 2, 6, 7, 9; ➢ Priorytet 7.: Doskonalenie jakości zadań realizowanych przez policjantów i pracowników Policji poprzez zapewnienie optymalnych warunków pełnienia służby/pracy: zadania 2, 4, 7, 8, 11, 12. • ***Strategia Bezpieczeństwa Narodowego RP*:** ➢ 3.2 Działania ochronne, p.87 Utrzymanie bezpieczeństwa i porządku publicznego; ➢ 4.3 Podsystemy ochronne, p. 4.3, Podsystemy ochronne, p. 133. • ***Sprawne Państwo 2020*:** ➢ Cel 7: Zapewnienie wysokiego poziomu bezpieczeństwa i porządku publicznego, podpunkt 7.1. • **Strategia bezpieczeństwa cybernetycznego Unii Europejskiej:** otwarta, bezpieczna i chroniona cyberprzestrzeń w zakresie zwiększenia zdolności operacyjnej w celu zwalczania cyberprzestępczości a także rozbudowy zasobów technologicznych na potrzeby bezpieczeństwa cybernetycznego. <u>W wyniku realizacji projektu możliwe byłoby :</u> • wzmocnienie roli polskiej Policji w wykrywaniu przestępstw komputerowych i cyberprzestępstw poprzez budowę unikalnego systemu o bardzo wysokiej wydajności dzięki zastosowaniu obliczeń rozproszonych, • innowacyjne wykorzystanie już istniejącej infrastruktury oraz zasobów informatycznych będących na wyposażeniu Policji, • wzmocnienie potencjału polskich organów ścigania w zakresie cyberbezpieczeństwa, • zacieśnienie współpracy pomiędzy organami ścigania: z systemu będą korzystały różne jednostki Policji (laboratoria kryminalistyczne, wydziały dw. z cyberprzestępczością KGP/KWP/CBŚP), • rozwinięcie polskiego potencjału badawczo-technologicznego. Technologią krytyczną niezbędną do prawidłowego wdrożenia projektu i jego skutecznej realizacji będzie opracowanie algorytmów związanych z obliczeniami rozproszonymi, pozwalającymi na dystrybuowanie zadań związanych z przełamywaniem jednokierunkowych funkcji skrótu pomiędzy dostępne komputery klienckie. **W wyniku zarówno zadań badawczych jak i prac rozwojowych przewidywany poziom gotowości technologicznej po zakończeniu projektu osiągnie poziom IX.**

<table>
<tr><td>5</td><td>Określenie, czy program strategiczny, program lub projekt ma być w całości realizowany przez jednego wykonawcę;</td><td>Projekt będzie realizowany w całości przez jednego wykonawcę, którym może być wykonawca wielopodmiotowy, tj. utworzone konsorcjum. Zaleca się, aby konsorcjum naukowe składało się z jednostek naukowych.</td></tr>
<tr><td>6</td><td>Określenie w formie harmonogramu, pożądanych terminów realizacji projektu, w tym jego etapów w szczególności podlegających rozliczeniu w ramach procesu nadzoru</td><td>Określenie pożądanego czasu trwania programu/projektu: do 48 miesięcy
<table>
<tr><th>Lp.</th><th>Nazwa zadania/ etapu badawczego</th><th>Okres realizacji [mies.]</th><th>Nazwa podzadania badawczego</th><th>Okres realizacji [mies.]</th><th>Opis/wynik etapu/zadania</th></tr>
<tr><td>1</td><td>ETAP I</td><td></td><td>Adaptacja i weryfikacja poprawności doboru istniejących rozwiązań informatycznych w zakresie badań wykorzystujących obliczenia rozproszone w stosunku do wymagań zachowania poufności i bezpieczeństwa informacji</td><td>6</td><td>W ramach tego podzadania przewidziana jest adaptacja i weryfikacja istniejących rozwiązań technologicznych, które za pomocą obliczeń rozproszonych korzystają z zastanych zasobów teleinformatycznych. Wynikiem zadania powinien być raport przedstawiający przydatność obecnych rozwiązań wykorzystywanych do prowadzenia obliczeń rozproszonych pod względem wymagań zachowania poufności i bezpieczeństwa informacji. Na tej podstawie powinny zostać sformułowane rekomendacje co do</td></tr>
</table></td></tr>
</table>

							kierunku prac nad docelową architekturą projektowanego systemu.	
					Opracowanie wymagań technicznych planowanej infrastruktury serwerowej	10	W ramach zadania koniecznym byłoby przeprowadzenie następujących prac projektowych: 1) Rozpoznanie istniejącej infrastruktury polskiej Policji (systemy operacyjne, infrastruktura sieciowa). 2) Opracowanie specyfikacji planowanego systemu serwerowego wraz z całą infrastrukturą.	
					Określenie wymagań dla narzędzi niezbędnych do zaprojektowania i realizacji oprogramowania serwerowego, aplikacji klienckiej oraz kopii zapasowych	8	W wyniku realizacji powinna zostać stworzona lista wymagań niezbędnych do zaprojektowania i realizacji oprogramowania serwerowego, aplikacji klienckiej oraz kopii zapasowych.	
					Opracowanie algorytmów obliczeń rozproszonych dla centralnego systemu do przełamywania zabezpieczeń	10	Wypracowanie algorytmów bazowych do budowy zaplanowanego oprogramowania i centralnego systemu do przełamywania	

							zabezpieczeń. Wynikiem tego zadania powinien być zestaw algorytmów, które zostaną wykorzystane w kolejnych zadaniach do zaprojektowania i implementacji oprogramowania.	
					Opracowanie założeń metodyk badawczych oraz programu badań	10	Wynikiem zadania powinien być raport zwierający listę założeń metodyk badawczych oraz programu badań.	
		2	ETAP II		Zaprojektowanie całościowej struktury systemu informatycznego do obsługi centralnego systemu przełamywania zabezpieczeń	14	Zadanie przewiduje skompletowanie niezbędnego sprzętu serwerowego (serwerów, okablowania, macierzy dyskowych i streamerów kopii zapasowych) oraz oprogramowania serwerowego. Efektem działania powinna być przygotowana infrastruktura serwerowa, która posłuży do implementacji centralnego systemu przełamywania zabezpieczeń.	
					Budowa całościowej struktury	14	Zadanie to przewiduje	

					systemu informatycznego do obsługi centralnego systemu przełamywania zabezpieczeń		budowę struktury niezbędnej do obsługi centralnego systemu do przełamywania zabezpieczeń. Prace powinny objąć połączenie wcześniej przygotowanego zestawu serwerów redundantnych ze stacjami klienckimi oraz stacjami administracyjnymi baz danych stacji klienckich i kolejek rozproszenia oraz systemem kopii zapasowych, na których dokonywane będą obliczenia mające na celu przełamywanie zabezpieczeń na szyfrowanych nośnikach cyfrowych.	
					Zaprojektowanie prototypu oprogramowania serwera oraz klienckiego	8	W ramach niniejszego zadania powinien zostać zrealizowany prototyp oprogramowania zarówno serwerowego do administracji całym systemem oraz oprogramowania klienckiego stacji roboczych wykonujących rozproszonych obliczeń i zwracając porcje danych do serwerów i systemu kopii	

							zapasowych.	
					Zaprojektowanie prototypu modułu oprogramowania serwerowego do administracji procesem przełamywania haseł dla zaszyfrowanych nośników	8	Celem tego zadania powinno być zaprojektowanie odpowiedniego modułu do istniejącego oprogramowania serwerowego, który posłuży do administracji procesem obliczeń i przełamywań zabezpieczeń z poziomu stacji roboczych laboratoriów kryminalistycznych, wydziałów ds. walki z cyberprzestępczością oraz innych zainteresowanych jednostek organów ścigania.	
					Zaprojektowanie i budowa prototypu oprogramowania do pozyskiwania danych z plików	8	Celem tego zadania powinno być zaprojektowanie architektury oprogramowania klienckiego instalowanego na stacjach klienckich	
					Opracowanie procedury walidacji centralnego systemu do przełamywania zabezpieczeń	8	Zadanie przewiduje opracowanie procedury walidacji całego systemu, jego oprogramowania oraz sprzętu. Wynikiem podetapu powinno być	

							opracowanie procedury dzięki której umożliwiony zostanie proces walidacji oraz testowania po wprowadzaniu zmian.	
					Walidacja metod badawczych	6	W ramach tego zadania powinna zostać przeprowadzona walidacja wykorzystanych metod badawczych oraz testy wytworzonego oprogramowania.	
					Test utworzonego oprogramowania	6	Przeprowadzenie testów wydajnościowych i jakościowych wytworzonego oprogramowania w środowisku testowym	
		3	ETAP III		Realizacja oprogramowania zarządzającego serwerem i infrastrukturą do wykonywania obliczeń rozproszonych za pomocą oprogramowania klienckiego	8	Wynikiem tego zadania powinna być realizacja oprogramowania zarządzającego dla serwera i aplikacji klienckich.	
					Realizacja modułu oprogramowania serwerowego do administracji procesem przełamywania haseł nośników	8	Wynikiem tego zadania powinno być oprogramowanie administracyjne pozwalające na sterowanie	

							procesem przełamywania haseł.	
					Realizacja oprogramowania do pozyskiwania danych z plików	8	Opracowanie algorytmów i oprogramowania pozwalającego na przeprowadzenie procedury ekstrakcji haszy z określonych typów plików	
					Realizacja oprogramowania klienckiego	6	Wynikiem tego zadania powinno być oprogramowanie aplikacji klienckiej.	
					Przeprowadzenie testów poprawności działania poszczególnych komponentów oprogramowania oraz całego systemu informatycznego	8	W wyniku realizacji tego zadania powinny zostać zidentyfikowane i usunięte potencjalne problemy w działaniu poszczególnych komponentów systemu jak i jego całości.	
					Opracowanie dokumentacji technicznej wykonanego oprogramowania i całego systemu informatycznego. Opracowanie procedur dostępu do baz danych oraz systemu zabezpieczeń przed nieuprawnionym dostępem	8	Wynikiem tego zadania powinna być dokumentacja wykonanego oprogramowania, procedur dostępu do baz danych oraz systemu zabezpieczeń.	

				Opracowanie metodyki i procedury dokonywania przełamywania zabezpieczeń za pomocą wykonanego centralnego systemu informatycznego	6	W wyniku realizacji niniejszego zadania badawczego powstać powinna metodyka oraz procedury przełamywania haseł z zabezpieczonych nośników.
		4	ETAP IV	Pilotażowe uruchomienie systemu informatycznego wykonanego w ramach niniejszego projektu z wykorzystaniem infrastruktury teleinformatycznej Policji oraz wykonanie prób przełamania obliczeń na testowych nośnikach cyfrowych.	10	W wyniku realizacji tego zadania możliwa będzie ocena wydajności systemu oraz jego przydatności w warunkach infrastruktury sieciowej zbliżonej do rzeczywistej oraz na bazie testowych zabezpieczonych nośników cyfrowych.
				Opracowanie metodyki i procedury dokonywania przełamywania zabezpieczeń za pomocą wykonanego centralnego systemu informatycznego	10	W ramach etapu powinna zostać opracowana szczegółowa procedura definiująca sposób zabezpieczania materiału mającego zostać poddanym atakom, sposobu ekstrakcji, przesyłania danych, sposobu zarządzania systemem, określania priorytetów oraz metodologii podejmowanych ataków.

		Projekt powinien być realizowany etapami, a każdy z etapów kończyć się osiągnięciem kolejnego poziomu gotowości technologii (PGT) zgodnie z wymogami określonymi w załączniku do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011r. w sprawie w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa (Dz. U. 2011 Nr 18, poz. 91). Pozytywny wynik etapów badań naukowych (zakończonych uzyskaniem VI PGT) potwierdzający możliwość skutecznego stosowania technologii determinującej powodzenie projektu oraz osiągniecie kluczowych funkcjonalności i parametrów zawartych w opisie projektu wraz z analizą możliwości i koncepcją jej rozwoju, jest warunkiem kontynuacji projektu i rozpoczęcia fazy rozwojowej. Szczegółowy harmonogram realizacji projektu zaproponuje wnioskodawca we wniosku o dofinansowanie projektu.
7	**Docelowy, główny użytkownik końcowy (gestor)**	Policja
8	**Ustalenie planu finansowego, w tym źródeł finansowania**	Projekt będzie finansowany ze środków NCBR, przewidzianych na finansowanie badań naukowych i prac rozwojowych na rzecz bezpieczeństwa i obronności i państwa (dotacja celowa). Wnioskodawca przedstawi we wniosku o dofinasowanie kalkulację kosztów realizacji projektu z podziałem na poszczególne lata. Planowany koszt realizacji projektu może być modyfikowany na podstawie wniosków złożonych przez wnioskodawców i w trakcie negocjacji przed zawarciem umowy.
9	**Ustalenie sposobu realizacji i zarządzania, w szczególności w zakresie organizacji kontroli, nadzoru i odbioru prac**	Wykonawca będzie realizował projekt i zarządzał nim w oparciu o uznaną metodykę zarządzania projektami np. PRINCE2. Dyrektor Centrum będzie sprawował nadzór nad realizacją projektu i może prowadzić kontrolę zgodnie z ustawą o NCBR, rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011r. w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa (Dz. U. 2011 Nr 18, poz. 91) oraz wewnętrznymi regulacjami NCBR w tym zakresie. Nadzór nad realizacją projektu jest prowadzony przez Zespół Nadzorujący, powołany przez Dyrektora NCBR. W skład zespołu nadzorującego wchodzą przedstawiciele ministra właściwego do spraw wewnętrznych, którzy pełnią w nim rolę ekspertów merytorycznych. Ekspertem wiodącym w zespole nadzorującym będzie przedstawiciel Komendanta Głównego Policji. Ekspert wiodący jest zobowiązany i uprawniony do przedstawiania jednolitego stanowiska Ministra Spraw Wewnętrznych i Administracji w toku negocjacji poprzedzających zawarcie umowy o wykonanie i finasowanie oraz w trakcie nadzoru nad realizacją projektu w NCBR.

		Proponowanym ekspertem wiodącym w zespole nadzorującym projekt w NCBR jest Instytut Służby Kryminalnej WBW WSPol w Szczytnie. Proponowanym podmiotem odpowiedzialnym za testowanie rozwiązań u przyszłego użytkownika w warunkach zbliżonych do operacyjnych lub/i w warunkach rzeczywistych - uprawniony do ustalenia programu badań i testów oraz innych spraw związanych z testowaniem jest Instytut Służby Kryminalnej WBW WSPol w Szczytnie. Dyrektor Centrum po uzyskaniu końcowej oceny merytorycznej projektu wykonanej przez Komitet Sterujący NCBR, dokona przyjęcia i oceny wyników projektu i uzna umowę o wykonanie i finasowanie projektu za wykonaną pod warunkiem wywiązania się wykonawcy z obowiązków dotyczących praw własności intelektualnej wynikających z ustawy i umowy.
10	**Prawa własności intelektualnej**	Właścicielem wynalazków, wzorów użytkowych i wzorów przemysłowych oraz autorskich praw majątkowych powstałych w wyniku wykonania Projektu zwanych dalej prawami własności intelektualnych (PWI) jest Skarb Państwa reprezentowany przez Komendanta Głównego Policji. Wykonawca będzie zobowiązany, na podstawie zawartej umowy o wykonanie i finasowanie projektu, do udzielenia licencji w zakresie odpowiadającym art. 32 ust. 3a powyższej ustawy na rozwiązania posiadane przez Wnioskodawcę lub przez niego nabyte, które ramach finansowania zostaną wykorzystane w celu realizacji projektu, a bez których nie byłoby możliwe korzystanie z rozwiązań powstałych w wyniku realizacji projektu. Wykonawca będzie zobowiązany do przeniesienia na Skarb Państwa własności prototypów oraz demonstratorów powstałych w wyniku wykonania projektu, bez prawa do dodatkowego wynagrodzenia (tj. w ramach otrzymanego na podstawie umowy przez Wykonawcę finansowania), na wyraźne żądanie Skarbu Państwa zgłoszone w terminie określonym w umowie o wykonanie i finansowanie projektu. Wykonawca projektu, na żądanie Skarbu Państwa lub Centrum, będzie zobowiązany do przekazać wszelką dokumentację dotyczącą PWI oraz rozwiązań posiadanych przez Wnioskodawcę lub przez niego nabytych w ramach finansowania, które zostaną wykorzystane w celu realizacji projektu, a bez których nie byłoby możliwe korzystanie z rozwiązań powstałych w wyniku realizacji projektu, w szczególności ich podstawowe założenia, opis techniczny, specyfikacje oraz wizualizacje, kody źródłowe, wynikowe, maszynowe i inne, dokumentację projektową, techniczną i eksploatacyjną. Dokumentacja musi być przekazana w formie umożliwiającej produkcję, eksploatację oraz utylizację.
11	**Zmiany w założeniach**	Niniejsze założenia do programu mogą być modyfikowane przez Komitet Sterujący do spraw badań naukowych i prac rozwojowych na rzecz bezpieczeństwa i obronności państwa przy realizacji jego zadań oraz przez Dyrektora Centrum na etapie inicjowania projektu oraz w trakcie nadzoru nad realizacją umowy o wykonanie i finasowanie projektu na podstawie opinii, rekomendacji Zespołu Nadzorującego lub Komitetu Sterującego, a w razie potrzeby ekspertów i w takim przypadku zmiany te nie wymagają uzgadniania z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych, którzy posiadają swoich przedstawicieli w Komitecie Sterującym.