BIURO BEZPIECZEŃSTWA NARODOWEGO

Czteroletni Przegląd Bezpieczeństwa Wewnętrznego USA, QHSR 2014

SYNTEZA

Departament Bezpieczeństwa Wewnętrznego USA (*Department of Homeland Security*, DHS) w czerwcu br. opublikował drugi w historii Czteroletni Przegląd Bezpieczeństwa Wewnętrznego (*Quadrennial Homeland Security Review*, QHSR). Według sekretarza bezpieczeństwa wewnętrznego Jeha Charlesa Johnsona *„QHSR 2014 określa priorytety dla bezpieczeństwa wewnętrznego na okres najbliższych czterech lat, w oparciu o ryzyka oraz nakreślenie dróg naprzód, celem zapewnienia skutecznego reagowania na szybko zmieniające się zagrożenia i niebezpieczeństwa"*[1]. Intencją DHS, która stanęła u podstaw publikacji dokumentu, jest zapewnienie, że przyszłe decyzje rządowe w zakresie bezpieczeństwa wewnętrznego podejmowane będą w sposób spójny, jednolity, przejrzysty i skoordynowany z działaniami innych departamentów oraz podmiotów posiadających kompetencje w dziedzinie bezpieczeństwa wewnętrznego.

Tegoroczny QHSR jest uzupełnieniem i kontynuacją pierwszej edycji dokumentu, wydanej w 2010 r. Potwierdza **pięć misji bezpieczeństwa wewnętrznego**, którymi są: zapobieganie terroryzmowi i wzmacnianie bezpieczeństwa wewnętrznego, zarządzanie i bezpieczeństwo granic, wdrażanie i egzekwowanie przepisów imigracyjnych, zabezpieczenie i ochrona cyberprzestrzeni oraz wzmacnianie narodowej gotowości i odporności. Wskazuje na odpowiedzialność władz wszystkich szczebli administracji państwowej, przedstawicieli prywatnego sektora i organizacji pozarządowych, za tworzenie sprzyjających warunków do podejmowania współpracy w ramach partnerstw publiczno-prywatnych, zapewnienie bezpieczeństwa publicznego, infrastruktury krytycznej i usług wspierających przygotowanie i reagowanie na zagrożenia.

[1] DHS Releases Second Quadrennial Homeland Security Review , http://www.dhs.gov/news/2014/06/19/dhs-releases-second-quadrennial-homeland-security-review (dostęp: 24 czerwca 2014 r.).

1) Główne części składowe QHSR 2014

Główne części składowe obejmują: podstawy prawne Przeglądu, cel Przeglądu, pięć rozdziałów merytorycznych oraz podsumowanie. Dokument uzupełniają dwa załączniki. Załącznik pierwszy opisuje kompetencje i zakres odpowiedzialności poszczególnych podmiotów państwa (instytucji i agencji rządowych wszystkich szczebli oraz obywateli i podmiotów prywatnych) w sferze bezpieczeństwa wewnętrznego. Załącznik drugi przedstawia proces przygotowania oraz poszczególne fazy opracowania QHSR.

2) Podstawy prawne Przeglądu

- Sekretarz bezpieczeństwa wewnętrznego jest zobowiązany ustawowo do przeprowadzania Czteroletniego Przeglądu Bezpieczeństwa Wewnętrznego[2]. W trakcie realizacji Przeglądu przeprowadza konsultacje z szefami innych departamentów i agencji federalnych, zwłaszcza z prokuratorem generalnym, sekretarzami stanu, obrony, zdrowia i służb społecznych, skarbu, rolnictwa oraz dyrektorem Wywiadu Narodowego (*Director of National Intelligence,* DNI), a także z kierownictwem DHS oraz innymi przedstawicielami władz wszystkich szczebli administracji państwowej, członkami Kongresu, przedstawicielami sektora prywatnego, środowiskami naukowymi i eksperckimi.

3) Cel Przeglądu

- Zakładanym celem QHSR jest nakreślenie ram strategicznych dla działań podmiotów wszystkich szczebli posiadających kompetencje w zakresie bezpieczeństwa wewnętrznego. Chodzi nie tylko o zapobieganie i przeciwdziałanie zagrożeniom, ale także o zapewnienie niezbędnych sił, środków i zasobów na rzecz bezpieczeństwa obywateli amerykańskich, ich własności oraz środków komunikacji ze światem (prawnych, migracyjnych, handlowych, związanych z przepływem osób i towarów oraz odbywaniem podróży).
- Opracowanie i opublikowanie QHSR to jeden z etapów zapewniania bezpieczeństwa wewnętrznego. Dokument zarysowuje wizję bezpiecznego

[2] Podstawa prawna QHSR: Sekcja 2401 Rekomendacji wdrożeniowych Ustawy z 2007 r. ws. Komisji 11 września, Pub. L. 110-53 (Section 2401 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53), stanowiąca poprawkę do Tytułu VII Ustawy z 2002 r. o bezpieczeństwie wewnętrznym (Title VII of the Homeland Security Act of 2002). Przepisy prawa zobowiązują Sekretarza Bezpieczeństwa Wewnętrznego do przeprowadzania Czteroletniego Przeglądu Bezpieczeństwa Wewnętrznego, począwszy od 2009 r. Pierwszy QHSR został zakończony i opublikowany w 2010 r. Tegoroczny QHSR został wydany z sześciomiesięcznym opóźnieniem.

państwa poprzez określenie zasadniczych misji w tej dziedzinie, priorytetowych celów dla każdego z obszarów misyjnych, tworzy niezbędne podstawy dla następnych etapów. Kolejnym etapem będzie dostosowane programów działania DHS i innych departamentów do ram strategicznych określonych w dokumencie. Ostatnim etapem tego procesu będzie przedłożenie budżetowe Sekretarza Bezpieczeństwa Wewnętrznego do Kongresu USA.

4) Najważniejsze tezy QHSR 2014:

a) Charakterystyka środowiska bezpieczeństwa

- Współczesne środowisko bezpieczeństwa USA cechuje się dużym stopniem niestabilności w kraju i zagranicą. Cięcia budżetowe oraz zagrożenie terroryzmem wpływają na klimat polityczny sprzyjający tworzeniu i wdrażaniu „spójnej, osiągalnej i realnej finansowo strategii" (*focused, achievable and affordable strategy*) rozwoju systemu bezpieczeństwa narodowego[3].
- Kluczowe czynniki ryzyka dla bezpieczeństwa wewnętrznego w ciągu najbliższych pięciu lat będą związane z następującymi wyzwaniami:
  - utrzymującym się wysokim poziomem zagrożenia terrorystycznego. Planowanie ataków i operacji terrorystycznych staje się coraz bardziej zdecentralizowane. Interesy Stanów Zjednoczonych, zwłaszcza w sektorze transportowym, wciąż mogą być celem ataku terrorystycznego;
  - wzrostem zagrożenia ataków w cyberprzestrzeni, co niesie za sobą większe ryzyka dla amerykańskiej gospodarki, zwłaszcza infrastruktury krytycznej;
  - wzrostem znaczenia zagrożeń o charakterze biologicznym, obejmujących m.in. bioterroryzm, pandemie lub choroby odzwierzęce, ze względu na wysokie prawdopodobieństwo ich zaistnienia oraz potencjalnie znaczące skutki;

[3] Zwrot wybrany z wypowiedzi kongresmana Jeffa Duncana (R-SC) w trakcie przesłuchania nt. QHSR w Komisji Bezpieczeństwa Wewnętrznego, DHS 2014 Quadrennial Review Urges Strategic Deployment Of Resources, by: Amanda Vicinanzo, Contributing Editor, HS Today.us, http://www.hstoday.us/briefings/daily-news-analysis/single-article/dhs-2014-quadrennial-review-urges-strategic-deployment-of-resources/5bb29d44ceaffd2b2f7ec3f6036bc76a.html (dostęp: 27 czerwca 2014 r.).

- terroryzmem jądrowym, ze względu na upowszechnienie improwizowanych środków przenoszenia, co znacząco zwiększa możliwość dokonania przestępstwa z użyciem ładunku jądrowego;
- wzrostem znaczenia i możliwości działania transnarodowych organizacji przestępczych, zajmujących się nielegalnym przerzutem osób i towarów, w tym narkotyków oraz handlem żywym towarem;
- wzrostem skutków, w tym kosztów, wynikających z zagrożeń naturalnych, tj. gwałtowne wyładowania atmosferyczne, powodzie, wichury lub związanych ze starzeniem się infrastruktury.

b) Zasady przewodnie (*guiding principles*)

- Zasady przewodnie stanowią podstawę dla poszczególnych priorytetów i tych obszarów działania, na które DHS położy nacisk. Zawierają się w następujących twierdzeniach:
  - podstawą bezpieczeństwa wewnętrznego jest zapobieganie terroryzmowi, przy czym system bezpieczeństwa wewnętrznego musi uwzględniać różne możliwe zagrożenia i ryzyka;
  - bezpieczeństwo wewnętrzne wspiera bezpieczeństwo gospodarcze;
  - bezpieczeństwo wewnętrzne wymaga wspólnoty sieciowej (tj. podmiotów, które są powiązane ze sobą rozlicznymi więzami i zależnościami, są świadome tych więzi i są gotowe współpracować ze sobą w sposób spójny i skoordynowany na rzecz wzmacniania bezpieczeństwa i realizacji wspólnych celów w tej dziedzinie);
  - bezpieczeństwo wewnętrzne jest zależne od rozwiązań i innowacji rynkowych;
  - bezpieczeństwo wewnętrzne stoi na straży prywatności, praw i swobód obywatelskich;
  - bezpieczeństwo wewnętrzne polega na zarządzaniu ryzykiem w taki sposób, aby koncentrować wysiłki na redukowaniu największych zagrożeń.

c) Priorytety strategiczne dla bezpieczeństwa wewnętrznego

- Zakłada się, że QHSR będzie przewodnikiem (*guidebook*) dla DHS oraz innych instytucji państwowych posiadających kompetencje w zakresie bezpieczeństwa wewnętrznego na rzecz spójnej i zintegrowanej realizacji pięciu misji Przeglądu[4]. Wspólne działania ukierunkowane będą

[4] Misje Przeglądu wymienione są w syntezie oraz opisane w kolejnych punktach niniejszej notatki.

w szczególności na następujące priorytety strategiczne dla bezpieczeństwa wewnętrznego:

- przeciwdziałanie zagrożeniom terrorystycznym (wzmacnianie zdolności DHS oraz innych instytucji państwowych do prowadzenia działań zagranicą) oraz zapobieganie terroryzmowi w kraju (analiza i pogłębianie wiedzy na temat czynników inspirujących do przeprowadzanie aktów terroryzmu, zintegrowanie służb kontrwywiadowczych, wzmocnienie partnerstwa służb ochronnych z wojskiem, zapewnienie szybkiego i efektywnego obiegu informacji, zapewnienie wsparcia podmiotów prywatnych i społeczeństwa dla podejmowanych działań);
- wzmocnienie cyberbezpieczeństwa poprzez likwidowanie tradycyjnych barier pomiędzy bezpieczeństwem fizycznym a bezpieczeństwem w cyberprzestrzeni, zwiększanie zdolności działania śledczych oraz wykorzystanie innowacyjnych technologii w cyberprzestrzeni na rzecz zabezpieczenia sieci rządowych i w sektorze prywatnym;
- zarządzanie ryzykiem wystąpienia zagrożeń biologicznych poprzez działania zapobiegawcze oraz w razie, gdyby było to niemożliwe, ograniczanie skutków ewentualnego ataku z użyciem środków biologicznych;
- przyjęcie podejścia polegającego na segmentacji ryzyka poprzez takie zarządzanie przepływem dóbr i osób, aby minimalizować zakłócenia, zapobiegać i ograniczać nielegalne przepływy finansowe, zwiększać wrażliwość instytucji państwa i społeczeństwa na potencjalne problemy rynkowe, uniemożliwiać przenikanie terrorystów, nowych chorób oraz inwazyjnych gatunków flory i fauny;
- wspomaganie realizacji misji poprzez rozwijanie sprawnych, innowacyjnych i skutecznych partnerstw publiczno-prywatnych;
- zapobieganie przenoszeniu środków jądrowych na terytorium USA;
- rozwijanie polityki imigracyjnej z uwzględnieniem nowych trendów migracyjnych oraz z poszanowaniem dla bezpieczeństwa publicznego;
- budowanie prężnych społeczności (*resilient communities*) poprzez wdrażanie Krajowego Systemu Gotowości (*National Preparedness System*)[5], w ramach całościowego podejścia do spraw zarządzania kryzysowego.

[5] *The National Preparedness System* to 10-stronicowy dokument opublikowany w listopadzie 2011 r. przez DHS, określający elementy składowe systemu gotowości na kryzysy i sytuacje

d) Zapobieganie terroryzmowi i wzmacnianie bezpieczeństwa (misja 1)

- Charakter zagrożenia terroryzmem dla bezpieczeństwa USA zmienił się w sposób zasadniczy po atakach 11 września 2001 r. i wciąż ewoluuje. Na skutek amerykańskich działań w ostatnich latach zmienił się charakter sprawowania przywództwa w Al-Kaidzie z centralistycznego w zdecentralizowany. Zagrożenie mogą też stanowić działania tzw. „samotnych wilków" oraz pojedynczych osób zainspirowanych ekstremistyczną ideologią. Rozproszony charakter zagrożenia skutkuje tym, że obecnie znacznie trudniej jest przewidzieć i zapobiegać potencjalnym atakom terrorystycznym wymierzonym w cele na terytorium USA.
- Strategiczne priorytety w zakresie zapobiegania i przeciwdziałania atakom terrorystycznym obejmują:
  - zidentyfikowanie, zbadanie i przeciwdziałanie zagrożeniom terrorystycznym tak szybko, jak to jest możliwe (priorytet ten obejmuje: wspieranie partnerów zagranicznych w zakresie zarządzania granicami, polityki celnej oraz zasobów i zdolności w zakresie egzekwowania prawa, wykorzystywanie informacji dotyczących niebezpiecznych osób lub towarów z odpowiednim wyprzedzeniem, tj. zanim przybędą one na terytorium USA);
  - „*zmniejszanie stogu siana*", tj. rozszerzanie bezpieczeństwa opartego na zarządzaniu ryzykiem (wdrażanie podejścia opartego na informacjach uzyskanych ze służb specjalnych, polegającego na wyprzedzających działaniach na rzecz przeciwdziałania ryzykom);
  - koncentrację działań na zwalczaniu agresywnych ruchów ekstremistycznych i zapobieganiu atakom, które mogą skutkować masową liczbą ofiar (w tym: wspieranie programów i inicjatyw służących zrozumieniu i budowaniu poszanowania dla przepisów prawa, prowadzenie powszechnych akcji uświadamiających zagrożenia oraz

---

kryzysowe, tj. identyfikację i ocenę ryzyk, ocenę poziomu zdolności niezbędnych do eliminacji ryzyk, utrzymywanie i rozwijanie nowych zdolności, elementy weryfikacji i kontroli postępów rozwijania systemu oraz sposoby osiągnięcia zasadniczego celu, jakim jest „*bezpieczny i odporny naród posiadający niezbędne zdolności do zapobiegania, ochrony, łagodzenia, przeciwstawienia się, odpowiedzi i odbudowy na wypadek wystąpienia zagrożeń i niebezpieczeństw, które stwarzają największe ryzyko*". Ryzyka obejmują m.in. katastrofy naturalne, pandemie, wycieki chemiczne oraz inne zdarzenia wywołane działalnością człowieka, ataki terrorystyczne i cyberataki.
Dostęp do dokumentu: http://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf
Źródło cytatu zawartego w niniejszym przypisie: http://www.fema.gov/national-preparedness-goal (dostęp: 27 czerwca 2014 r.).

okoliczności, które mogą poprzedzać przeprowadzenie ataku terrorystycznego);
  - zmniejszanie liczby potencjalnych celów ataku (zwiększanie zakresu ochrony infrastruktury krytycznej, w tym obiektów o znaczeniu symbolicznym i infrastruktury drogowej oraz imprez masowych, a także liderów państwa, poprzez przeciwdziałanie możliwości użycia improwizowanych ładunków wybuchowych lub innych materiałów, które mogą znaleźć zastosowanie jako broń oraz takie oddziaływanie na zachowania potencjalnych agresorów, aby zwiększać efekt odstraszania przed dokonaniem aktu terroru);
  - integrowanie danych i analiz (w tym: poprawa efektywności wykorzystywania danych wywiadowczych, z poszanowaniem dla praw ludzkich i obywatelskich Amerykanów).
- Istotnym elementem przeciwdziałania terroryzmowi jest zapobieganie nielegalnemu rozprzestrzenianiu materiałów chemicznych, biologicznych, radiologicznych i nuklearnych oraz środków ich przenoszenia. Cel ten wymaga szczególnie szybkiego przewidywania, identyfikowania i likwidowania zagrożeń w tym zakresie. Za szczególnie ważne uznane zostały zagrożenia biologiczne, obejmujące m.in. bioterroryzm, pandemie, przenikanie chorób obcego pochodzenia, ekspansję obcych gatunków flory i fauny, skażenia żywności i wody, a także zagrożenia biotechnologiczne oraz wynikające ze wzrostu obrotów handlowych. Działania w tym zakresie skoncentrowane będą na:
  - zapobieganiu i powstrzymywaniu wystąpienia zamierzonych lub niezamierzonych zagrożeń biologicznych w USA;
  - poprawie procesów podejmowania decyzji poprzez zapewnienie decydentom wszystkich szczebli w DHS oraz partnerom odpowiedniej wiedzy na temat zagrożeń biologicznych;
  - wczesnym wykrywaniu i priorytetowym reagowaniu na incydenty biologiczne;
  - poprawie zaufania i zachęcaniu partnerów DHS do działania;
  - skutecznym reagowaniu na incydenty biologiczne;
  - utrzymywaniu funkcji niezbędnych do realizacji misji w trakcie oraz po wystąpieniu incydentu biologicznego.

e) Zarządzanie i bezpieczeństwo granic (misja 2)

- Środowisko bezpieczeństwa ostatnich lat cechuje znaczący wzrost przepływu osób i towarów w skali globalnej. Zjawiskom tym towarzyszy wzrost nielegalnego tranzytu przez granice. DHS oraz inne instytucje federalne są zobowiązane tak zarządzać granicami oraz przepływem osób i towarów przez granice USA, aby wpływać na poprawę sytuacji gospodarczej państwa i ograniczać ryzyka związane z możliwą działalnością przestępczą w tym obszarze (tj. eksport terroryzmu, przepływ towarów i technologii niebezpiecznych lub wrażliwych, nielegalne obroty finansowe i handlowe, nielegalne migracje motywowane względami klimatycznymi lub politycznymi, napływ obcych chorób, a także obcych gatunków flory i fauny).
- Misja zarządzania i bezpieczeństwa granic realizowana będzie poprzez zapobieganie nielegalnym transakcjom i obrotom handlowym, wprowadzanie dodatkowych zabezpieczeń legalizacyjnych dotyczących transferu osób i towarów przez granice USA, osłabianie i demontaż transnarodowych organizacji przestępczych. Działania instytucji państwowych w tym obszarze skoncentrowane będą na:
  - wprowadzaniu segmentacji ruchu, obliczonej na promowanie legalnego przepływu osób i towarów oraz zawężaniu przestrzeni dla zjawisk niepożądanych, w tym przestępczych;
  - poprawianiu jakości oraz ochrony infrastruktury transportowej na granicach (w portach lotniczych i morskich oraz na lądzie), tak aby sposób zarządzania granicą przyczyniał się do zwiększania przepływu osób i towarów, a tym samym dalszej poprawy sytuacji gospodarczej państwa, zgodnie z interesami bezpieczeństwa, prawem handlowym USA oraz zasadami konkurencyjności;
  - rozwijaniu partnerstw publiczno-prywatnych celem określenia wspólnych interesów i zasobów na rzecz poprawy wspólnego bezpieczeństwa oraz określenia potrzeb w tym zakresie.

f) Wdrażanie i egzekwowanie przepisów imigracyjnych (misja 3)

- Misja ta obejmuje dwa zasadnicze cele: wzmocnienie i efektywne administrowanie systemem imigracyjnym oraz zapobieganie nielegalnym migracjom. W związku z tym:
  - promowana będzie imigracja legalna oraz integracja legalnych imigrantów w ramach społeczeństwa amerykańskiego;
  - rozwijana będzie efektywność administrowania systemem służb imigracyjnych;

- podjęte będą dalsze wysiłki na rzecz zapobiegania nielegalnym przekroczeniom granicy oraz osłabienia nielegalnej imigracji;
- będą zatrzymywane, aresztowane i wydalane w szczególności te osoby, które mogą stanowić zagrożenie dla bezpieczeństwa narodowego, bezpieczeństwa publicznego lub w zakresie ochrony granic.

g) Zabezpieczenie i ochrona cyberprzestrzeni (misja 4)

- Zagrożenia w cyberprzestrzeni obejmują m.in. kradzieże własności intelektualnej, ataki hakerskie na witryny internetowe ważnych instytucji państwowych i publicznych oraz na obiekty infrastruktury krytycznej. DHS ściśle współpracuje z rządem i partnerami z sektora prywatnego w zakresie zwiększania zdolności służących zapobieganiu i zwalczaniu działań przestępczych w cyberprzestrzeni, wspiera rozwój gospodarczy oraz rozwój nowych technologii i upowszechnia informacje służące poprawie cyberbezpieczeństwa.
- Wzrasta liczba i rodzaj zagrożeń cybernetycznych dla infrastruktury krytycznej. Różne obiekty w sektorach energetycznym, transportowym, wodnym lub finansowym są celami coraz bardziej skomplikowanych ataków cybernetycznych, co może skutkować negatywnymi konsekwencjami dla amerykańskiego stylu życia, wartości i ekonomii.
- Strategiczne priorytety w zakresie zabezpieczania i ochrony cyberprzestrzeni obejmują:
  - wzmacnianie odporności i bezpieczeństwa infrastruktury krytycznej (poprzez upowszechnianie wiedzy na temat istoty zagrożeń w cyberprzestrzeni oraz stosowanie całościowego podejścia służb państwowych i obywateli w podejmowanych działaniach na rzecz zapobiegania, zniechęcania potencjalnych agresorów, ochrony i reagowania na incydenty w cyberprzestrzeni, a także badania tych zagrożeń i szybkiej odbudowy);
  - wspieranie *Federal Civilian Government Information Technology Enterprise* celem koordynowania programów rządowych dot. zakupów nowych cybertechnologii, zmniejszania kosztów tych zakupów, wyposażenia sieci rządowych w nowoczesne narzędzia chroniące dane oraz zapewnienia, że rządowe inicjatywy i programy w zakresie ochrony cyberprzestrzeni będą stale rozwijane i wdrażane;
  - wzmocnienie egzekwowania prawa i efektywności reagowania na incydenty w cyberprzestrzeni;
  - wzmocnienie całego ekosystemu (rozwijanie i wdrażanie nowoczesnych zabezpieczeń, procesów standaryzacyjnych i kodeksów dobrych praktyk

w cyberprzestrzeni w kraju i za granicą, metodyczne kształcenie personelu zdolnego do efektywnego wdrażania inicjatyw i programów rządowych dotyczących ochrony cyberprzestrzeni, rozwijanie współpracy międzynarodowej w tym zakresie).

h) Wzmacnianie narodowej gotowości i odporności (misja 5)

- Wzmacnianie narodowej gotowości i odporności na zagrożenia realizowane będzie poprzez wspólny, skoordynowany wysiłek instytucji rządowych, organizacji pozarządowych, przedsiębiorstw prywatnych i obywateli. W trakcie realizacji tej współpracy zasadne jest wykorzystywanie istniejących modeli partnerstw publiczno-prywatnych (w tym: mechanizmów koordynacji działań oraz wymiany informacji i danych, regulacji standaryzacyjnych i motywacyjnych, związków operacyjnych, zasad wspólnego inwestowania i produkcji, doświadczeń z przeszłości, istniejących kodeksów dobrych praktyk). USA będą identyfikować i likwidować luki w istniejących systemach zabezpieczeń, wzmacniać system zarządzania kryzysowego oraz kłaść nacisk na szybką odbudowę po ewentualnym wystąpieniu kryzysu.
- Wzmacnianie systemu zarządzania kryzysowego będzie polegać na inwestycjach na rzecz szybkiego dostarczania i obiegu precyzyjnej informacji, uruchomieniu efektywnych zunifikowanych systemów reagowania na zdarzenie, dostarczaniu na czas odpowiedniego wsparcia oraz zapewnieniu efektywnej komunikacji kryzysowej. Proces odbudowy będzie polegał w pierwszym rzędzie na odrestaurowaniu podstawowych funkcji w rejonie dotkniętym kryzysem. W drugiej kolejności odbudowa będzie ukierunkowana na wdrożenie głównych wniosków wynikających z kryzysu, tak aby społeczeństwo dotknięte jego skutkami stawało się silniejsze, mądrzejsze i bezpieczniejsze, niż przed kryzysem.

i) Proces przygotowania oraz poszczególne fazy opracowania QHSR

- Tegoroczny 104-stronicowy QHSR jest uzupełnieniem i kontynuacją pierwszej edycji dokumentu, wydanej w 2010 r., w której ustanowiono pięć zasadniczych misji oraz zdefiniowany został zakres pojęciowy „bezpieczeństwa narodowego". Na tej podstawie w drugim QHSR zdefiniowane zostały priorytetowe obszary przyszłych działań resortu i władz federalnych w obszarze bezpieczeństwa wewnętrznego.
- Prace nad drugim QHSR zostały podzielone na cztery fazy. Faza przygotowawcza (od 2012 do początku 2013 r.) polegała na określeniu

zagrożeń i ryzyk w sytuacji dynamicznych zmian zachodzących w środowisku bezpieczeństwa oraz zarysowaniu koniecznych korekt celów służących realizacji pięciu misji bezpieczeństwa wewnętrznego. W fazie studiów i analiz (wiosna–lato 2013 r.) realizowane były studia i analizy szczegółowe, ukierunkowane na konkretne problemy. Faza opracowywania dokumentu i podejmowania decyzji (jesień 2013–początek 2014 r.) była okresem uzgadniania najważniejszych decyzji z innymi departamentami i agencjami federalnymi oraz innymi partnerami zaangażowanymi w tworzenie QHSR, w tym priorytetyzacji celów i przyszłych działań organów państwa w zakresie bezpieczeństwa wewnętrznego. Ostatnia faza podsumowująca polegała na skumulowaniu wysiłków celem ostatecznego opracowania redakcyjnego, wydania i przesłania dokumentu do Kongresu USA.

- Funkcję sekretariatu QHSR pełniło – analogicznie jak podczas opracowywania pierwszego Przeglądu – Biuro ds. Strategii, Planowania i Analiz, wchodzące w skład Biura ds. Polityki Departamentu Bezpieczeństwa Wewnętrznego USA.

Opr. Sławomir Kamiński