Internal Audit Report

Audit of the Incident Command System

Project 6B307

Date: March 2021

Final Draft Audit Report for Presentation to the
Departmental Audit Committee

Canada

Introduction

The Internal Audit Directorate (IAD) conducted an audit of Fisheries and Oceans Canada's (the Department) use of the Incident Command System (ICS) in accordance with the departmental 2019-2021 Risk-Based Audit Plan.

The Canadian Coast Guard (Coast Guard) is a Special Operating Agency (SOA) within the Department. The Coast Guard's response mandate is derived from the *Oceans Act*, the *Canada Shipping Act* and the *Arctic Waters Pollution Prevention Act.* In this regard, Coast Guard has the legislative authority to ensure an appropriate response to ship source and mystery pollutant spills in Canada's area of responsibility. Further, working closely with the Canadian Armed Forces, Coast Guard has a leadership role in the overall management of the Maritime Search and Rescue (SAR) System. At the tactical level, Coast Guard is responsible for the coordination of the on-water SAR response. The Coast Guard also supports other government departments during incidents and emergencies through the provision of experienced personnel, ships, aircraft and other maritime services.

In March 2013, the Government of Canada announced the World Class Tanker Support System (WCTSS) – a suite of initiatives to strengthen maritime safety through prevention, preparedness and response measures to protect the public and the environment. These included modernizing Canada's navigation system and measures to clean up oil and other spills. As part of its commitments to the WCTSS, the Coast Guard adopted the Incident Command System (ICS) as the Agency-wide incident management methodology.

The Incident Command System is an internationally recognized incident management methodology used for the command, control, and coordination of emergency response operations. The methodology is designed to enable effective, efficient incident management by integrating equipment, personnel, procedures, and communications in order to operate within a common organizational structure. It helps to ensure the safety of the responder, the achievement of response objectives and the efficient use of resources.

The Coast Guard implemented its adoption of ICS in 2018 and it became the basis for its response methodology to meet its incident response responsibilities and mandate, as well as to realize several benefits, including:

- Helping to ensure effective command and control regardless of the nature, scope, scale or complexity of an incident through standard approaches throughout a response to an incident;
- Strengthening the internal capacity for its mandated response operations and all-hazard incidents;
- Increasing interoperability with response partners;
- Using command structures that are adaptable to various incident categories and types;
- Identifying positions that are best suited to fulfill Incident Command Post (ICP) positions and the resources (personnel and equipment) required to respond to an incident;
- Developing training standards to help ensure that personnel receive appropriate training; and
- Providing benchmarks against which to observe and learn from incident response operations.

In December 2019, the Coast Guard initiated a re-organization of its response programs under the Response Branch with the goal of defining its incident response strategy, establishing response priorities, and aligning response personnel and assets.

At the time of this audit, the Department of Fisheries and Oceans (DFO) had not adopted the Incident Command System as its incident response and incident management approach and methodology.

Why this audit is important

The 2019-2020 Fisheries and Oceans Canada Corporate Risk Profile identified emergency management as a key risk area. The Incident Command System was identified for audit to assess departmental readiness to respond to incidents in light of differing response capacity, the remoteness of sites, and the varying types of incidents that can arise. The Department, and specifically the Canadian Coast Guard, responds annually to a broad variety of all-hazard maritime incidents in both a primary and supporting Agency role.

Audit Objective

The objective of this audit was to determine whether the Department's use of the Incident Command System supports effective incident response planning, command, coordination, outcomes, reporting, and resource management.

Scope and Approach

The audit examined: incident response governance in place within the Department; whether the Incident Command System was used as prescribed during an incident response operation, including communications and reporting; and whether lessons learned activities are conducted following an incident response operation.

The audit did not undertake a review of Coast Guard personnel and equipment capacity or requirements relative to its incident response operation activities. The audit also did not examine the role of other response partners involved with the Coast Guard and DFO during incident response operations.

The audit covered the period April 1, 2019 to March 31, 2020 but the audit did consider information outside of this period in specific case studies.

The audit was carried out at Fisheries and Oceans Canada National Headquarters (NHQ) and selected Coast Guard regional offices, which involved:

- 85 Interviews with Coast Guard incident response personnel from NHQ and all regions, and site visits to Western, Central & Arctic and Atlantic regions;
- 26 Interviews with DFO regional directors general and selected regional staff involved in departmental incident response operations from all DFO regions; and
- Case study analysis from selected Coast Guard and DFO incident response operations.

Annex A presents the lines of enquiry and supporting criteria that were used to conclude against the audit objective.

Conclusion

Overall, the audit concluded that the Coast Guard is using the Incident Command System (ICS) to support effective incident response planning, command, coordination, outcomes, reporting and resource management.

The audit identified opportunities for improving incident response management including:

- Increasing collaboration between Coast Guard National Headquarters and the regions to:
    - Define Coast Guard's incident response strategy and priorities;
    - Develop a training strategy in both official languages to build Agency-wide incident response and incident management preparedness capacity and capability; and
    - Implement an online ICS information management system to facilitate incident decision-making, documentation, communication, and interoperability with response partners.
- Improving incident response operation cost monitoring and cost recovery processes;
- Adhering to prescribed ICS and Incident Command Post information and communications protocols to help ensure timely response communications within the Department, to the media and the public; and
- Clarifying lessons learned guidance and process to improve the consistency and value of incident response after action reporting.

Statement of Conformance

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing as supported by the results of the Quality Assurance and Improvement Program of Fisheries and Ocean Canada's Internal Audit Directorate.

Governance

The audit examined whether the Department had a governance framework that defines and communicates accountabilities, roles and responsibilities of those involved in incident command activities.

Given that DFO has not adopted the Incident Command System (ICS), the audit examined governing incident command activities within the Canadian Coast Guard. DFO's experience with the ICS along with the specific opportunities for the Department are discussed at the end of this section.

Guidance has been developed to support Coast Guard response personnel in the use of the Incident Command System

The audit found that the Coast Guard's Incident Management Handbook (IMH, 2015) and Incident Command System Plan for Incident Management (2015) define specific incident response operation roles, responsibilities and command structures. Although the IMH is not a formal policy instrument, it is the primary reference tool used to guide Coast Guard personnel in the use of the ICS during response operations.

Opportunities exist to increase collaboration between Coast Guard National Headquarters and the regions to achieve Agency-wide response and incident management priorities

As previously noted, the Coast Guard initiated a re-organization of its response programs under the Response Branch in December 2019 with the goal of defining its incident response strategy, establishing response priorities and aligning response personnel and assets.

Coast Guard regional personnel cited a collaborative and constructive working relationship with NHQ and the Office of Incident Management (OIM). Regions recognize that demands on the OIM are high to deliver numerous ICS priorities and are well positioned to support OIM in the delivery and achievement of these priorities given they:

- Respond to hundreds of incidents annually, covering a broad range and type of incidents; and
- Are the primary front-line developers of ICS and understand the strategic and tactical requirements of Incident Command Post structures and roles in coordination with other federal, provincial, territorial, municipal and other response partners.

Interviews with incident response stakeholders across Coast Guard regions identified the following opportunities for collaboration to support NHQ Response Branch in delivering Agency-wide response and incident management priorities:

1. Defining Coast Guard's Agency-wide incident response and incident management strategy and priorities.

At present, the Response Branch is identifying Agency-wide response and incident management priorities. The audit noted that incident response operations are not funded through a dedicated Coast Guard program; therefore, strategic priorities could help to ensure that response program mandates are achieved. Otherwise, program personnel, assets and equipment may not be aligned to priority areas resulting in the risk of operational ineffectiveness and inefficiency.

As a proactive measure, Western Region has developed a regional incident management plan to align its response program resources under a single response program similar to the one envisioned by the Response Branch. While neither Central & Arctic nor Atlantic regions have developed their own regional plans, they indicated they might eventually do so in the absence of an agency-wide incident management strategy.

2. Prioritizing the implementation of an online ICS information management system.

The audit found that the Coast Guard does not have an online information system in place to facilitate the management of incident response operations or which is capable of interoperability with its response partners. For several years, Coast Guard has been developing an online system to be used within an Incident Command Post. However, the audit found that the online system has not been prioritized for implementation agency-wide.

This finding is important for the Coast Guard because rather than using an online information system similar to other federal, provincial, territorial, municipal and industry response partners within an ICS-based ICP, Coast Guard regions use ICS paper-based forms to document daily ICP decision-making and resource management (personnel, equipment, operational costs, etc.). Coast Guard regional personnel noted that reliance on paper-based forms decreases operational efficiency and slows the flow of information within the ICP, to regional management and to NHQ.

As a lead federal response agency, having an online system could help to enhance Coast Guard's interoperability with its response partners, which is a primary Coast Guard objective in using the ICS as its incident response methodology.

Coast Guard ICS training supports incident response and incident management preparedness

The audit examined the Coast Guard's ICS training program and whether training courses and simulation exercises are effective in helping ensure personnel are prepared to respond to an incident.

Within the Coast Guard, ICS training is centrally planned and coordinated at NHQ by the Office of Incident Management to help ensure that training is provided in a manner consistent with ICS standards.

Coast Guard personnel from all regions noted that overall, ICS course training and incident response simulation exercises help to ensure preparedness to participate in or lead an incident response operation, and provide a balance between mandate areas such as environmental response (for example, oil spills), and a broader range of non-mandated incidents (for example, floods and forest fires).

The audit noted Coast Guard training and exercising practices, including:

- Conducting the Goletas and CANUSLANT exercises in 2019. The September Goletas exercise in Port Hardy, British Columbia, focused on a major maritime disaster and environmental response with the United States Coast Guard, provincial and First Nations response partners. The June CANUSLANT exercise focused on a major environmental response to an oil spill and involved provincial and First Nations response partners;
- Senior cadets at the Coast Guard College are receiving introductory level ICS course training through an initiative led by NHQ-OIM ; and
- NHQ, Western and Atlantic regions maintain an inventory of personnel with ICS course training who have participated in ICS exercises and incident response operations.

However, a strategic training approach has not been adopted to build Agency-wide ICS-based incident response and incident management preparedness capacity and capability.

Through interviews with Coast Guard regional personnel from all regions, the audit found that a strategic training approach has not been adopted Agency-wide to build ICS-based incident response preparedness capacity and capability within the Coast Guard.

The audit identified the following opportunities for improvement:

1. *An Agency-wide inventory of personnel with ICS training and experience could support the deployment of incident response personnel.*

Although NHQ, Western and Atlantic regions maintain an inventory of personnel with incident response experience, there is no dedicated single database or system to help ensure the accuracy and completeness of the information. Coast Guard used to maintain a National Training Tracking Tool (NTTT) to compile records of course completion and training by personnel. However, the NTTT ceased to meet user needs and has not been used since 2018. One of the potential uses of an online ICS information management system would be to maintain an inventory of ICS trained and experienced personnel. An Agency -wide database could help to identify personnel who are best suited to be deployed to an incident response operation and to fulfill key ICP roles. Otherwise, there is a risk of mobilizing and deploying inexperienced personnel that could result in ineffectiveness within an ICP and impact the incident response operation.

2. *Some ICS training could be provided by Coast Guard personnel.*

Coast Guard ICS training is funded and managed through the NHQ-OIM. Through interviews with Coast Guard regional personnel, it was noted that NHQ could explore the feasibility of accrediting regional personnel to provide ICS training. Experienced regional incident response personnel noted an opportunity to leverage regional incident response experience towards delivering ICS courses internally. The audit found there are few Coast Guard members who have been accredited to provide ICS training courses and workshops. Instead, most ICS training is provided by external providers. Travel is often required for personnel to attend training courses, for which costs could potentially be avoided if there were regional instructors instead.

The OIM confirmed that course delivery opportunities have been provided in the past to interested and experienced regional incident response personnel. The OIM acknowledged that the development of a formal accreditation process is underway with the regions.

3. *ICS training content is currently not standard, available or consistent in both official languages.*

The audit found that since the implementation of ICS within Coast Guard, the limited availability of ICS materials in French, such as the Incident Management Handbook, ICP position profiles and training course and workshop materials, have created barriers to using ICS. NHQ-OIM is presently working with Central Region to update training courses and content to help ensure their consistency in both official languages.

These findings are important for the Department because while ICS training provides value for personnel who receive training, there exist limitations within current Coast Guard training approaches. These limitations not only create barriers to accessing and applying training but can also impact the Department's ability to help ensure the right personnel are identified for training and are prepared to participate effectively in an incident response operation.

The Incident Command System is not the standard Departmental incident response and management approach

While the audit scope was limited to examining the effectiveness of the Incident Command System, the audit identified a broader risk for the Department that affects incident management resulting from the lack of a common approach across the Department.

In contrast to the Coast Guard, DFO has not adopted the ICS as its incident response and management approach. DFO's current approach is based on NHQ and regional emergency management plans and business continuity plans (BCPs) designed to maintain critical service delivery and activities, and achieve the timely recovery of other services and activities. The audit found that, to date, the differing incident response and

management approaches within the Department have been based on the relatively few incidents requiring the involvement of both DFO and the Coast Guard.

The Big Bar rockslide incident and salmon recovery operation in the summer of 2019 highlighted the impact of using different incident response approaches within the Department. At the onset of the response operation, DFO was the lead federal responder in collaboration with the province of British Columbia and First Nations stakeholders. Throughout the Big Bar response operation, DFO regional personnel were able to provide scientific advice in relation to salmon protection strategies. DFO regional management proactively requested the assistance of the Coast Guard to support the ICP operation because its regional personnel did not possess the required level of ICS ICP experience to assume the lead response role within the ICP or fulfil key ICP roles. Moreover, during the Big Bar operation, DFO faced scrutiny and criticism from response partners and in media reporting which impacted DFO's reputation and credibility. DFO and Coast Guard personnel cited that the Coast Guard's support helped to stabilize the Department's lead federal role within the ICP and improve collaboration with the province and First Nations stakeholders.

DFO regional directors general, affected DFO assistant deputy ministers, and Coast Guard Assistant Commissioners indicated agreement that there is an opportunity for DFO to adopt the Incident Command System and an ICS training program in collaboration with the Coast Guard given its expertise with the ICS. Doing so could:

- Increase DFO's incident response capacity and capability, as well as improve interoperability with the Coast Guard and other response partners; and
- Build the Department's overall incident management and response capacity and capability.

The Big Bar incident is important to note because using different incident response and management approaches may be a risk to the Department as it may present less than optimal conditions for DFO and the Coast Guard to collaborate effectively or efficiently, limit their interoperability and opportunity to leverage their respective knowledge and expertise during an incident response operation, and could create conditions for ineffective response operations leading to reputational harm for the Department. That said, this finding lies outside the audit scope, as it relates to overall departmental incident response and management as opposed to ICS specifically, and more audit work may be required to assess this risk to the Department based on the examination of additional incidents where DFO and the Coast Guard worked together. This risk could become the subject of future audit work.

Recommendations:

1. The Coast Guard Deputy Commissioner, Operations, in collaboration with the Assistant Commissioners, should:
   a) Define Coast Guard's Agency-wide incident response and incident management strategy and priorities; and
   b) Develop a training strategy in both official languages to build Agency-wide incident response and incident management preparedness capacity and capability.

2. The Coast Guard Deputy Commissioner, Operations should implement an online ICS information management system to facilitate incident decision-making, documentation, communications, and interoperability with response partners.

Management of Incident Processes

The audit examined whether the Department uses the ICS to plan how it: responds to an incident; activates resources (personnel and materiel); and executes activities required for incident response consistently, and in compliance with regulations, across the regions. Given that DFO is not a primary user of the ICS and its limited experience using the ICS, the audit focused on how the Coast Guard uses the ICS.

Coast Guard regions are establishing incident command structures consistent with prescribed guidelines to manage incident response operations and support interoperability with response partners.

The audit examined how Coast Guard regions establish the type of incident command structure to manage incident response operations, whether these are established as prescribed by the Coast Guard ICS and ICP guidelines, and whether these command structures support coordination and collaboration with response partners.

Within the ICS, there are two primary command structures: Single Command and Unified Command. In a Single Command structure, the role of the Incident Commander (IC) is held by one individual from the lead response organization. Under Unified Command, the role of the Incident Commander is shared by two or more individuals from their respective response organizations.

The audit found that the Coast Guard regions are establishing incident response command structures as prescribed by the Coast Guard's Incident Management Handbook and in consideration of their regional environments to achieve a successful response outcome. Although the selection of incident command structures varies by region, they were found to be consistent with the ICS principle of interoperability among response partners and the Coast Guard's goal of helping ensure effective overall command, coordination, and aligned response efforts regardless of the scope, scale and complexity of an incident.

Coast Guard personnel are assessing incidents and deploying response resources as required by Coast Guard ICS guidance

The audit examined how the Coast Guard uses the ICS to assess incidents, and to identify and deploy the resources (personnel and equipment) required to respond to an incident. Annually, the Coast Guard responds to hundreds of incidents – each requiring the deployment of personnel and equipment. Through interviews and case studies, the audit found that regional personnel are assessing incidents as prescribed by the Incident Management Handbook by using ICS forms to assess an incident's type (severity) and identify resource requirements.

Across and within regions, viewpoints varied on whether using ICS-based planning activities enable an efficient deployment of resources. Some regional personnel noted that the Coast Guard adopts the ICS principles of flexibility, adaptability and scalability to expand and contract an incident response structure and operation as required. Others noted risks of initially over deploying personnel and equipment leading to shortages for other regional response operations.

Through review of Coast Guard ICS guidance documents and interviews with regional response personnel, the audit found that resource deployment risks are lower for type 5 and 4 incidents as they require fewer personnel, whereas type 3, 2 and 1 incidents require significantly more personnel and equipment.

The specific resource characteristics for each type of incident are described below.

Incident Type (complexity)		
	1	This type of incident is the most complex requiring national resources for safe and effective management and operation.
	2	This type of incident extends beyond the capabilities for local control and is expected to go into multiple operational periods. A type 2 incident may require the response of resources out of area, including regional and/or national resources to effectively manage the operations, command and general staffing. The National Incident Management Team (NIMT) shall be activated.
	3	When the incident exceeds capabilities, the appropriate ICS positions should be added to match the complexity of the incident. Command staff and general staff functions are activated only if needed. The incident may extend into multiple operational periods (days).
	4	Command staff and general staff are activated only if needed. The incident is usually limited to one operational period (day) in the control phase.
	5	The incident can be handled with one or two single resources with up to six personnel. The incident is contained within the first operational period (day) and often resolved within an hour to a few hours after resources arrive on scene.

This finding is important for the Department because should the Coast Guard continue to act as the lead departmental responder for all incidents, including those where DFO could provide support, there is a higher risk that regional Coast Guard personnel may not be available to respond to incidents in their regions. This finding is also important because recent type 3 incidents have highlighted limits within the Coast Guard's response capacity (number of available experienced personnel and assets, including equipment and vessels) and capability (competency of personnel who understand ICS requirements and have experience using ICS during incident response operations), including:

- During the Big Bar rockslide and salmon recovery operation in the summer of 2019, the Coast Guard was called on by DFO to support the Department's response role. However, the Coast Guard did not have sufficient personnel within Western Region to respond; therefore supporting personnel were deployed from Central & Artic and Atlantic regions. Atlantic region stated that they do not have the capacity to respond to a type 2 incident such as Big Bar.
- In April 2015, Coast Guard experienced limits with both personnel and vessel capacity and capability while managing the *Brigadier General M.G Zalinski* oil spill operation followed shortly by the need to respond to the *MV Marathassa* oil spill operation. Both responses were classified as type 3 incidents.

As indicated in the audit scope, the audit did not undertake a review of Coast Guard personnel and equipment capacity or requirements relative to its incident response operation activities. The risk inherent within incident response resource decision-making and deployment was not found to be an indication of personnel or equipment shortages within the Coast Guard or due to the Coast Guard's use of the ICS. Rather, the audit found that Coast Guard regions are managing these inherent incident risks relative to their regional resource capacity and the number of incidents to which they respond.

The audit noted that Western Region had been operating as a single response program prior to the recent agency-wide re-organization under the NHQ Response branch. The early adoption of the single program model has facilitated the identification and deployment of the best-positioned personnel and equipment across response program areas (for example, environmental response, search and rescue) and branches (for example, Fleet). In doing so, Western Region is managing the risk of resource shortfalls when deploying personnel and equipment to regional response operations.

Incident response operation cost monitoring and cost recovery processes require improvement

The audit examined how the Coast Guard is tracking incident response operation costs for internal reporting and in support of cost recovery claims to the Ship Owner Pollution Fund (SOPF). Established under Part 7 of the *Marine Liability Act*, the SOPF is a Canadian account mandated to review claims and reimburses costs related to ship-source pollution in Canadian waters. The Canadian compensation regime is based on the principle that the ship owner is liable for pollution damage. However, to receive compensation, claimants must demonstrate that reasonable response costs and prevention measures have been taken. The Coast Guard has made claims to the SOPF for the recovery of incident response operation costs.

The Coast Guard's Environmental Response Cost Recovery Manual states that regions are responsible for providing all pertinent incident response operation cost information and consistently applying costing principles to enhance the Coast Guard's credibility and better ensure a good offer on claims. However, the audit found that there was limited capacity in financial management within the regions given there was only one Cost Recovery Analyst (CRA) per region responsible for collecting response operation cost information for all incidents, and preparing cost recovery claim submissions to the SOPF. CRAs noted that they often must follow-up with personnel and contractors for several months following the conclusion of an incident response operation to obtain cost related information and documents. CRA's and NHQ also confirmed there is no central process to monitor agency-wide costs for all incident response operations. Rather, incident response costing is monitored regionally and not reported to NHQ.

Interviews with CRAs, regional personnel and NHQ confirmed that the SOPF and ship-owners are increasingly challenging the Coast Guard's justification of personnel and equipment costs throughout the response operation. For the period 2017-2019, the Coast Guard submitted $2,544,729 in claims for environmental response operations and recovered $1,840,362 for a recovery rate of 72%, leaving $704,366 in non-reimbursed expenses assumed by the Coast Guard. Through interviews with NHQ, regional CRAs and review of the SOPF settlement offers, the audit found that these costs were not reimbursed primarily due to the absence of supporting Coast Guard cost information and documentation.

These findings were attributed to:

- Inconsistent and/or limited presence of financial management experience within an Incident Command Post to help ensure accurate, complete and timely reporting of response operation costs. This finding was operational in nature and was not attributed to roles and responsibilities within the Department's Chief Financial Officer Sector;
- No central process to monitor agency-wide incident response costs; and
- No oversight or review process to help ensure that cost recovery claim submissions are supported by complete information prior to being sent to the SOPF.

These findings are important because without a complete and accurate accounting of incident response operation costs, the Coast Guard may not be able to:

- Monitor and report on the total cost of incident response operations, as well as forecast personnel and equipment levels needed to meet regional response requirements; and more critically,
- Recover claim submissions resulting in operational deficits.

Recommendation:

3. The Coast Guard Deputy Commissioner, Operations, in collaboration with the assistant commissioners, should implement measures to improve the accuracy, completeness and timeliness of incident response operations costs to support internal monitoring, reporting and cost recovery claim submissions.

Incident Communications and Reporting

Coast Guard information dissemination protocols are not consistently adhered to, resulting in a lack of timely response operation communications within the Department, to the media and to the public.

The audit examined the processes and protocols in place for communicating and reporting on incident response activities. Per required by Coast Guard ICS and ICP protocols, the Incident Commander is responsible for authorizing the release of response operation information internally and externally regardless of the size or complexity of the incident. The Coast Guard's Incident Management Handbook notes that successful mission execution may not equate to a successful response operation if there are failures to manage public perceptions of the response – before, during, and after operations.

The audit found that when adhered to, prescribed Coast Guard protocols help to facilitate the provision of timely response operation information updates internally within the Department and externally to response partners, the media and the public. When incidents of a more serious type occur, regional and national incident management teams (RIMT and NIMT) are often involved with regional and national communications branches. As the number of actors and demand for information increases, so does the time required to release information.

The audit noted examples of incidents where the Incident Commander did not retain authority for the dissemination of information to the media and public. In these incidents, authority was assumed by Coast Guard and DFO National Headquarters (NHQ), which increased the time required to obtain approved communications for the media and public – ranging between several hours in most instances and two days in another. During these incidents, local media were receiving response operation updates from other federal, provincial, territorial and municipal response partners while the Coast Guard was internally approving communications messaging. These incidents proved challenging for regional communications staff who are responsible for managing media and community relationships because NHQ did not authorize them to provide tactical, non-sensitive information responses to the media until Coast Guard and DFO senior management were briefed and approved the release of response operation updates.

These findings are important because, in a social media environment, the Department risks harm to its credibility as a lead federal incident response organization, and a loss of the public's confidence in its ability to successfully respond to incidents should incident response information not be provided to the media and public in a timely manner.

Recommendation:

4. The Coast Guard Deputy Commissioner, Operations, in collaboration with the Assistant Commissioners, should:
    a) Help ensure adherence to prescribed Incident Command System information protocols during an incident response operation to support the timely internal and external communication of accurate information; and
    b) Identify what types of information can be readily shared externally by regional communications personnel and what types should be sensitive and treated accordingly.

Lessons learned guidance and processes could be clarified to improve the consistency and value of incident response operation reporting

The audit examined how the Department reports on the outcomes of incident response operations and conducts post-response lessons learned activities. The audit found that across all Coast Guard regions, some form of lessons learned activity is undertaken following the conclusion of an incident response operation, including verbal debriefs and/or a formal report. When completed, lessons learned activities provide valuable insight and promote a continuous learning culture to improve future incident response training, exercises and operations. The audit also found that incident reporting is not completed consistently and that further guidance is needed on when and how to prepare lessons learned reports.

The Coast Guard has established guidance for when and how to prepare lessons learned reports for Type 3, 2 or 1 incident response operations. However, there are no requirements to complete lessons learned reports for Type 5 or 4 incidents. While these incidents are smaller in terms of response complexity and operational scale, they represent the majority of incidents the Coast Guard responds to annually and can yield observations on how to improve how future incident response operations.

The primary reason noted by regional response personnel for not completing lessons learned reports consistently is the time required to complete, communicate, validate and finalize the report. With regional response employees dedicating their time to response operations, completion of lessons learned reports following the conclusion of an incident are not prioritized for completion relative to ongoing operational requirements.

The audit also found that across and within regions and NHQ, there is no central or common repository approach or system to store lessons learned reports. An archive of lessons learned reports was noted by regional response personnel as having value to document how the Coast Guard has responded to incidents and to identify successful practices as well as areas for improvement.

The audit noted efforts in Coast Guard Western region to complete and communicate reports in less time through the MS Teams tool and to capture outcomes, lessons learned and recommendations for improving future incident response operations. The NHQ-OIM plans to update lessons learned guidance and also incorporate into its incident exercise framework, planning process and manual. Given Coast Guard regions respond to hundreds of incidents annually, they are well-positioned to collaborate with NHQ-OIM on updating lessons learned guidance and processes.

These findings are important because a culture of continuous improvement can help the Department improve its incident response preparedness capabilities. Improved incident response preparedness capabilities can help increase the likelihood of successful incident response operations as well as the confidence of Canadians in the Department as a lead federal response organization.

Recommendation:

5. The Coast Guard Deputy Commissioner, Operations should update guidance and processes to improve the consistency and value of incident response after action reporting.

Annex A: Lines of Enquiry and Audit Criteria

The audit criteria were developed based on the following sources:

- *Canadian Coast Guard Incident Command System Framework*
- *Canadian Coast Guard Incident Command System Plan for Incident Management*
- *Canadian Coast Guard Incident Command System Overview*
- *Canadian Coast Guard Incident Management Handbook*
- *Canadian Coast Guard Environmental Response Cost Recovery Manual*

Audit Criteria by Lines of Enquiry	Conclusion
Line of Enquiry 1: Governance	
Criterion 1.1: The Department has a governance framework in place at National Headquarters and in the regions that clearly defines and communicates accountabilities, roles and responsibilities of those involved in incident command activities.	Partially Met
Line of Enquiry 2: Management of Incident Processes	
Criterion 2.1: The Department uses the ICS to plan how it: responds to an incident; activates resources (personnel and materiel); and executes activities required for incident response consistently, and in compliance with regulations, across the regions.	Partially Met
Line of Enquiry 3: Incident Communications and Reporting	
Criterion 3.1: The Department has processes and protocols in place for communicating and reporting on incident response activities.	Partially Met
Criterion 3.2: The Department reports on the outcomes of incident response and conducts post-response lessons learned activities.	Partially Met

Annex B: Recommendations and Management Action Plans

Recommendations	Management Action Plan
1. The Coast Guard Deputy Commissioner, Operations, in collaboration with the Assistant Commissioners, should: a) Define Coast Guard's and Agency-wide incident response and incident management strategy and priorities; and b) Develop a training strategy in both official languages to build Agency-wide incident response and incident management preparedness capacity and capability.	*Management agrees with the recommendations* 1.a) DC Operations will define the Agency's incident response and incident management strategy by updating the ICS Plan for Incident Management. This will include greater clarity of command and control structures during responses to incidents, outline incident command resources, and align them to maximize the Agency's ability to effectively respond to maritime incidents. Further, DC Operations will develop Agency-wide priorities for incident management. *Target date: March 31, 2022* 1.b) DC Operations will develop a training strategy, building on the successes of ICS training approach conducted during initial implementation, thereby ensuring that enhancements are made to the ICS/IM approach to training in both official languages. *Target date: December 2022*
2. The Coast Guard Deputy Commissioner, Operations should implement an online ICS information management system to facilitate incident decision-making, documentation, communications, and interoperability with response partners.	*Management agrees with the recommendation* DC Operations will develop an Incident management system, comprised of a tool or suite of tools to enhance interoperability with key partners including Indigenous communities. *Target date: March 2023*
3. The Coast Guard Deputy Commissioner, Operations, in collaboration with the Assistant Commissioners, should implement measures to improve the accuracy, completeness and timeliness of incident response operations costs to support internal monitoring, reporting and cost recovery claim submissions.	*Management agrees with the recommendation* As on ongoing task, DG Response will ensure continuous improvements are made related to the accuracy, completeness and timeliness of incident response cost tracking, reporting and cost recovery claim submissions, through the following initiatives: ▪ Incorporating financial guidance in national & regional orders for Coast Guard incident response. *Implementation status as at March 2021:* *Completed. The Coast Guard has provided evidence of incorporating financial guidance in national and regional*

	incident response orders. ▪ Improving training for financial staff in the incident management team. *Target date: this item is liked to MAP response #1b) with a target date of December 2022.* ▪ Improving cost recovery tools, templates and guidelines for claims submitted to the Ship-source Oil Source Pollution Fund (SOPF). *Implementation status as at March 2021:* *Completed. The Coast Guard has provided evidence of updated standard guidelines and practices for cost recovery claim submissions to the SOPF.* ▪ Continuing to host ongoing bilateral meetings between Coast Guard Response staff and SOPF staff. *Implementation status as of March 2021:* *Completed. The Coast Guard has provided evidence that engagement mechanisms have been initiated and meetings have been held with the SOPF to improve the quality of cost recovery claim submissions.*
4. The Coast Guard Deputy Commissioner, Operations, in collaboration with the Assistant Commissioners, should: a) Help ensure adherence to prescribed Incident Command System information protocols during an incident response operation to support the timely internal and external communication of accurate information; and b) Identify what types of information can be readily shared externally by regional communications personnel and what types should be sensitive and treated accordingly.	*Management agrees with the recommendation* DC Operations will work closely with DG Communications to develop a Coast Guard specific, crisis communications protocol to identify what type of information can be shared externally during an incident, and to facilitate its timely and accurate release to the media and public. *Target date: March 2022*
5. The Coast Guard Deputy Commissioner, Operations should update guidance and processes to improve the consistency and value of incident response after action reporting.	*Management agrees with the recommendation* DC Operations will enhance continuous improvement/lessons learned processes and procedures to inform future exercises and training activities, thereby improving mission readiness. *Target date: March 2023*