

**DEPARTMENT OF JUSTICE CONSULTATION
REFORMING THE LAW ON FOREIGN INTERFERENCE**

COMMENTS

OF

CANADIAN TELECOMMUNICATIONS ASSOCIATION

FEBRUARY 2, 2024

Introduction

1. The Canadian Telecommunications Association is please to provide its comments to the Department of Justice's consultation on reforming the law on foreign interference"¹ (Consultation).
2. The Canadian Telecommunications Association is an industry association dedicated to building a better future for Canadians through connectivity. Our members include service providers, equipment manufacturers, and other organizations in the telecommunications ecosystem, that invest in, build, maintain and operate Canada's world-class telecommunications and broadcasting networks. Through our advocacy initiatives, research, and events, we work to promote the importance of telecommunications to Canada's economic growth and social development, and advocate for policies that foster investment, innovation, and positive outcomes for Canadians who rely on telecommunications and related services.
3. In this submission we do not comment on all the issues raised in the consultation. While the Canadian Telecommunications Association may comment on other issues in further stages of the Consultation, our comments in this reply focus primarily on questions posed under Issue # 3 in the Consultation, Whether to Modernize Canada's Sabotage Offence. In addition, to the extent that any comments in this intervention conflict with a comment of an Association member, the comment of the member shall prevail with respect to that member.

Modernizing Canada's Sabotage Offence

Q1. (Part 1) Should the law of sabotage be updated to ensure it covers modern forms of critical infrastructure such as water, sewage, energy, fuel, communication, and food services?

4. The law of sabotage should be updated to make clear that it covers modern forms of critical infrastructure, including telecommunications and broadcasting facilities. As explained in the Consultation, acts of sabotage can target a wide range of assets. Such assets include information and communications networks and technology, which together play a key role in the delivery and support of daily necessities for Canadians, are vital to their safety and security, and are integral to the maintenance of Canadian democracy.

¹ [Reforming the law on foreign interference – Online public consultation \(justice.gc.ca\)](https://www.justice.gc.ca/consultations/2018/foreign-interference)

5. This concern has already motivated the Government of Canada to take important policy and legislative action. In placing restrictions on the use of certain foreign-made telecommunications equipment by telecommunications service providers, the government emphasized the role that telecommunications play in ensuring the safety and security of Canadians:

Given the greater interconnectedness and interdependence of 5G networks, a breach or exploitation in this environment would have a more significant impact on the safety and security of Canadians and Canadian critical infrastructure than in previous network generations. In order to reap the economic and social benefits of 5G technology, Canada must continue to secure the foundation of its telecommunications system and adapt to the changing technological and threat environment.²

6. In introducing Bill C-26³, *An Act Respecting Cybersecurity, amending the Telecommunications Act and making consequential amendments to other Acts*, the government once again stressed the importance of protecting telecommunications and other critical infrastructure from modern threats:

In the 21st century, cyber security is national security – and this new legislation will ensure that Canada's defenses meet the moment. Most importantly, it will help both the public and private sectors better protect themselves against cyberattacks. This bill is one part of our robust strategy to defend Canada and the crucial infrastructure that Canadians rely on.

7. The current *Criminal Code* offence of sabotage (Section 52) does not expressly recognize the importance of protecting these modern forms of infrastructure. It specifically mentions traditional forms of assets, such as “vessels, vehicles, aircraft, machinery, [and] apparatus” and also includes non-specific reference to a general category of infrastructure comprising “other thing[s]”. While the words “or other thing” is arguably sufficient to cover modern forms of infrastructure, there remains the risk that a court could restrict the meaning of “thing” to assets that fall within the same general category of vessels, vehicles, etc. and does not include important elements of critical modern-day infrastructure, such as information and communications networks, technology, software and data.
8. In considering how to amend Section 52 to cover critical infrastructure, one can look at the approaches taken in other countries. As cited in the Consultation, Australia recently replaced two sabotage offences contained in its *Crimes Act 1914* (Crimes Act) with seven new offences in its *Criminal Code* (Division 82)⁴ (Australia Law). While the previous offences in the Crimes Act were limited to acts

² <https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement-securing-canadas-telecommunications-system.html>

³ <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading>

⁴ National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018
<https://www.legislation.gov.au/C2018A00067/latest/text>

against defence property, the new sabotage offences cover acts of sabotage against ‘public infrastructure’, which definition notably includes both infrastructure operated by the state and infrastructure owned and operated by the private sector.

9. The Australia Law defines ‘public infrastructure’⁵ as “any infrastructure, facility, premises, network or electronic system” that belongs to the Commonwealth (of Australia), is defined in referenced defense-related statutes, or “*any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act 1997.*” [emphasis added] Public infrastructure also includes any infrastructure, facility, premises, network or electronic system that “provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind” that is located in Australia and “belongs to or is operated by a constitutional corporation or is used to facilitate constitutional [i.e. interstate] trade and commerce.” Again, this definition includes privately-owned entities that support inter-state trade.
10. UK recently enacted its *UK National Security Act*⁶ (UK Act) which, among other things, creates an offence of sabotage (Section 12). Unlike the Australian sabotage offence, which limits its scope to specific types of public and private sector infrastructure, the UK offence employs a general definition of “assets”, which are defined to include “an asset of any kind whether tangible or intangible and includes in particular real and personal property, electronic systems and information.” Therefore, under the UK Act, sabotage consists of conduct that damages any “asset”, is “prejudicial to the safety or interests of the United Kingdom” and is conducted for, on behalf of, or for the benefit of a foreign power (the foreign power condition). Sabotage can occur whether the conduct takes place, and whether the asset is, in the UK or elsewhere.
11. Although the Australia Law expressly identifies types of assets that are protected, there remains the risk, however small, that something that should be protected would be found to fall outside of the definition of protected “public infrastructure”. Conversely, the sabotage offence in UK Act is appropriately not limited by the type of asset that is damaged or otherwise compromised, but rather is premised upon whether such conduct is harmful to the safety or interests of the country. This provides greater flexibility and future-proofs the law such that it can cover new types of infrastructure and assets that become important to the country’s safety security. For example, mobile wireless networks and technologies were not considered critical infrastructure in the early 1980s, while today they clearly are. At the same time, as discussed below, the UK sabotage offence is linked to a benefit to a foreign power – a narrowing condition for sabotage which is not currently part of Canada’s Criminal Code offence and which the Canadian Telecommunications Association would strongly oppose, were such a condition to be proposed in Canada.

⁵ Ibid. Definition in Section 82.2.

⁶ National Security Act 2023, <https://www.legislation.gov.uk/ukpga/2023/32/section/12>

12. While privately-owned communications infrastructure would fall within either of the approaches taken under the Australia Law and UK Act, we recommend that Canada's government adopt a broad definition of infrastructure and assets covered by the law such as the one used in the UK Act, but also include a non-exhaustive list of key critical infrastructure and assets that are meant to fall within such definition. This would leave no doubt as to the type of present-day infrastructure and assets that the government intends to protect from acts of sabotage, and also provide the legislation with the flexibility needed to cover other types of infrastructure and assets that may become critical to the safety of Canadians or the national interest in the future.
13. For example, the updated law could cover 'assets' defined as:
- ...an asset of any kind whether tangible or intangible and includes in particular real and personal property, electronic systems and information, including, without limitation:
- (i) any part of a telecommunications facility within the meaning of the *Telecommunications Act*;
 - (ii) any part of a broadcasting undertaking within the meaning of the *Broadcasting Act*;
 - (iii) *[other identified critical infrastructure]*
14. In addition, because of the decentralized nature of information and communications technologies and networks, the updated Canadian sabotage offence should, like the UK Act, expressly state that the offence covers assets whether they are in Canada or elsewhere.
15. Moreover, the *status quo* in Canada's current sabotage offence, whereby the offence applies without regard to whether the sabotage is undertaken for the benefit of a foreign power, should be maintained – consistent with Australia's approach. Given the profoundly harmful effects of acts of sabotage and related acts, the offence should not be limited to instances in which a foreign state is the beneficiary. Beneficiaries could include foreign or domestic non-state actors, and even an individual.

Q1. (Part 2) Should [the law of sabotage] be updated to clarify that it covers a broader range of negative impacts on infrastructure?

16. The law of sabotage should be updated to clarify that it covers a broader range of negative impacts on infrastructure and other assets. The current sabotage provisions under Section 52 of the Code cover any act or omission that (emphasis added):
- 2(a) **impairs the efficiency or impedes the working** of any vessel, vehicle, aircraft, machinery, apparatus or thing; or

(b) **causes property**, by whomever it may be owned, **to be lost, damaged or destroyed**.

17. While these negative impacts may have been sufficient at the time Section 52 was enacted, they are too limited to cover all the potential negative impacts that can occur as a result of the sabotage of modern-day infrastructure, such as information and communications networks and systems. For example, taking over control or denying rightful access to a computer system, or taking over a broadcasting network, would likely not be considered an impairment of its efficiency or impeding it from working, nor would it necessarily result in the asset being lost, damaged, or destroyed.
18. Once again, we can look to the recent Australia Law and UK Act to see references to a wider range of negative impacts that are covered under their sabotage laws. The Australia Law covers “damage to public infrastructure” (which, as noted, includes privately-owned telecommunications infrastructure) which is described as conduct that:
- (a)...destroys it or results in its destruction;
 - (b) ...involves interfering with it, abandoning it, resulting in it being lost or rendered unserviceable;
 - (c) ...results in it suffering a loss of function or becoming unsafe or unfit for its purpose;
 - (d) ...limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it;
 - (e) ...results in it or any part of it becoming defective or being contaminated;
 - (f)the conduct significantly degrades its quality;
 - (g) if it is an electronic system – the conduct seriously disrupts it.
19. The UK Act provides a non-exhaustive list of negative impacts under its definition of ‘damage’:
- 12(1)(3) “damage” includes any of the following (whether permanent or temporary) –
- (a) destruction;
 - (b) alteration;
 - (c) contamination;
 - (d) interference;
 - (e) loss of or reduction in access or availability;
 - (f) loss of or reduction in function, utility or reliability.

20. We recommend that the government update the law of sabotage to cover the type of negative impacts that can occur when modern forms of critical infrastructure are targeted, such as those included in the Australia Law and UK Act.

Q1. (Part 3) Or, would it be enough to rely on existing offences such as unauthorized use of computer; mischief; use of an explosive or other lethal device against a government or public facility, public transportation or other infrastructure?

21. While some acts or omissions that negatively impact Canada's national interest may fall within the scope of the above referenced existing offences, it is not enough to simply rely on these offences. An important element of sabotage that is absent from these other crimes is that sabotage targets the national interest. This makes sabotage a more serious crime than ordinary computer crimes or mischief, and as we argue below, suitable for the application of greater penalties.
22. Updating and clarifying the law of sabotage also sends a powerful message of deterrence, dissuading individuals or entities from engaging in acts of sabotage against critical infrastructure due to the potential legal consequences. Confidence in the public and international trading partners is also strengthened when they know that laws are comprehensive and up-to-date, reinforcing trust in Canada's national security strategy and the reliability of critical infrastructure, such as telecommunications systems.

Q2. Would it be beneficial to give the judge the ability to increase the penalty, when sentencing an individual, if the crime was committed for the benefit of a foreign entity?

23. As noted above, the updated law of sabotage should cover acts that address crimes committed for the benefit of, or that involve a foreign entity, as well as crimes that prejudice the national interest but were not committed for the benefit of, or involve, a foreign entity. Given the serious nature of sabotage, in both cases the government should impose penalties greater than those prescribed under the current law.
24. The crime of sabotage in Canada currently carries a maximum penalty of imprisonment for a term of not more than 10 years, irrespective of whether the crime was committed for the benefit of or with the involvement of a foreign entity. While 10 years is a significant sentence, it is notably much less than the penalties for acts of sabotage under recently enacted laws in countries such as Australia and the UK – even where a particular offence does not involve a foreign principal.

25. The Australia Law creates seven offences with varying penalties:

Table 1: Australian Sabotage Offences

Offence	Section	Penalty
Sabotage – involving foreign principal with intention as to national security	82.3	25 years
Sabotage – involving foreign principal reckless as to national security	82.4	20 years
Sabotage – with intention as to national security	82.5	20 years
Sabotage – reckless as to national security	82.6	15 years
Introducing vulnerability – with intention as to national security	82.7	15 years
Introducing vulnerability – reckless as to national security	82.8	10 years
Preparing for or planning sabotage	82.9	7 years

26. The most serious offence (s.82.3) carries a penalty of 25 years imprisonment and requires both intent to prejudice national security and that the conduct be “engaged in on behalf of, or in collaboration with, a foreign principal or a person acting on behalf of a foreign principal” or be “directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal.” Section 82.4 is like section 82.3 in that it requires the element of foreign involvement, but the prosecution only must prove recklessness and not intent to prejudice the national interest.
27. The remaining offences do not require that they be conducted on behalf of a foreign principal (or any other foreign involvement as required in Sections 82.3 and 82.4) only that they prejudice national security.⁷
28. In creating these tiers of offences, the Australia Law recognizes acts of sabotage on behalf of or involving foreign entities as the most serious type of sabotage and imposes greater penalties for these types of offences. Nevertheless, other sabotage offences carry penalties that significantly exceed the current maximum penalty for sabotage in Canada.
29. Unlike the Australia Law, the UK Act does not create separate offences and its offence of sabotage requires that the conduct be carried out for or on behalf of a foreign power. This can include conduct instigated by, under the direction or control of, with financial or other assistance provide by, or carried out in collaboration or with agreement of, a foreign power. In recognizing the seriousness of foreign motivated sabotage, the UK Act imposes a penalty of imprisonment for life or a fine (or both).

⁷ Sections 82.5 and 82.6 offences also include an optional element of conduct that will “advantage the national security of a foreign country.”

30. While their laws of sabotage are different, both Australia and the UK impose much greater penalties for sabotage on behalf of or involving foreign entities than the current laws in Canada. As suggested in the Consultation, Canada's existing criminal law does not fully reflect the serious impact of foreign interference and Canada's offence of sabotage should include greater penalties for acts conducted on behalf of or involving foreign entities.
31. That said, it is extremely important - given that acts of sabotage against infrastructure can cause significant harm to national security even if there is no foreign involvement - that Canada increase penalties even where a foreign party is not involved or does not benefit. These domestic acts of sabotage should, as is the case with the law of sabotage in Australia, carry penalties that are greater than the maximum of 10 years of imprisonment under existing Canadian law.
32. We further support the idea in Australia Law that creates companion offences for recklessness⁸ and for the planning of an act of sabotage⁹.

Q3. (Part1) Are the existing exemptions from liability still appropriate? Should other exemptions be considered, like those found in the terrorism provisions of the Criminal Code?

33. Subsection 52(3) of the Code provides that a person has not committed an act of sabotage by reason only that he stops work because of a failure of him or his bargaining agent to agree with his employer on any manner relating to his employment, or as the result of stopping work in combination with other workmen or employees for their own reasonable protection.
34. While it is reasonable to protect employees from liability for lawful work stoppages, any such exemption should make clear that an individual involved in a legal work stoppage cannot escape liability if they commit any act or omission with the intention of prejudicing the national interest, including the safety or security of Canada.
35. Just as employees should benefit from a saving provision in connection with lawful work stoppages, the owners and operators of critical infrastructure require protection from liability for actions or omissions that are attributable to work stoppages by their employees. For example, if Bill C-58 were to become law, the owner's or operator's ability to maintain the operation of and protect its critical infrastructure in the face of a replacement worker ban and overly narrow maintenance of activities agreement may be compromised. As such, the updated sabotage law should expressly state that owners and operators of such infrastructure have not committed an act of sabotage if the act or omission in question is attributable to the work stoppage and the employers' inability to use

⁸ Section 82.4 and 82.6. *Ibid.*

⁹ Section 82.9 *Ibid*

replacement workers to an extent necessary to maintain the integrity, efficiency, or functionality of its critical infrastructure.

36. It is also important to provide appropriate exemptions from liability to private sector owners and operators of critical infrastructure, and their authorized personnel, when their acts or omissions are made in good faith or because of a government, court, or administrative tribunal order.
37. Telecommunications networks are complex interconnected systems, and no provider is immune to outages. In addition to natural disasters and power outages, network failures can result from human error, such as mistakes made during maintenance, upgrades, or routine operations. The accidental cutting of cables, misconfigurations or failures in equipment or other errors can also cause disruptions in service.
38. The Australia Law includes an appropriate “good faith” defence to potential liability. It provides that it is a defence to prosecution if the person who commits the act is the owner or operator of, or acting on behalf of, or with the consent of, and the owner or operator of the public infrastructure, and engaged in conduct in good faith, the conduct is within the lawful authority of the owner or operator, and the conduct is reasonable in the circumstances for the purpose of exercising that lawful authority.¹⁰ A similar defence should be incorporated into an updated Canadian sabotage law.
39. In addition to the good faith defence, owners and operators of infrastructure should be exempt from liability for acts or omissions that are required by law or order of a government, court or administrative tribunal. For example, the federal government has introduced Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*¹¹ which, in the case of telecommunications, would give the Governor-in-Council and the Minister broad powers to order a telecommunications service provider to, among other things, remove products from its facilities, suspend the provision of services, prohibit the upgrading of any product, or terminate a service agreement with a third party equipment or software provider.
40. While Bill C-26 requires that such orders be made only when the government considers it is necessary to secure Canadian telecommunications systems, it does not require the government to consider the other impacts that could result from complying with such orders, which could create unintended harms and negatively impact the operation of telecommunications networks. Network owners and operators and their personnel should not be liable under sabotage laws for complying with orders of government, courts or administrative tribunals.

¹⁰ S.82.10(2).

¹¹ Bill C-26, <https://www.parl.ca/legisinfo/en/bill/44-1/c-26>

Q3 (Part 2) Should there be a requirement to get the consent of the Attorney General to proceed with the offence?

41. There should be no requirement to obtain the consent of the Attorney General to proceed with a prosecution for the offence of sabotage. There are very few offences under the *Criminal Code* that require the consent of the Attorney General before proceeding with a prosecution. For example, because terrorism-related offences encompass acts carried out for political, religious or ideological purposes, objectives or causes, there may be concern that officials could use anti-terrorist laws to target people based on their race, religion, or political beliefs. The requirement to obtain consent from the Attorney General before proceeding with terrorism offences is intended to prevent such abuse.
42. However, requiring consent of the Attorney General is susceptible to similar concerns of abuse. The Attorney General is a political appointee, and requiring consent of a political appointee runs counter to the principle of prosecutorial independence. The process can become victim to political interference and may make law enforcement reluctant to investigate and seek charges for such offences. While a consent requirement may be appropriate for crimes that require that they be committed in support of a belief or cause, sabotage is not such an offence. Sabotage is not concerned with a person's beliefs or causes, rather it is concerned with the impact of the conduct.

Q4. Would it be appropriate to create an offence to capture possession of a device to commit sabotage? Should such an offence require intent to commit sabotage? What kinds of devices would be appropriate to include in such an offence?

43. We agree that it would be appropriate to create a companion offence to capture possession of a device to commit sabotage. The *Criminal Code* already contains possession of device offences, such as possession of a device to obtain unauthorized use of computer (section 342.2); mischief (section 430); and delivering explosive or other lethal device used against a public place, government facility, or a public transportation system or infrastructure facility an (section 431.2). Adding a possession of a device to commit sabotage would be consistent with the approach taken with these other offences and provide additional deterrence to dissuade individuals and entities from committing or preparing to commit acts of sabotage.
44. If an updated offence of sabotage were to be broadened to cover a wide array of critical infrastructure it will be difficult to create an exhaustive list of devices that should be included in the possession offence. One approach would be to include any device, or part of a device, including computer software, designed or adapted primarily to commit an offence of sabotage or that the persons intend to use or has used to commit an act of sabotage. Such an approach is consistent with the way devices are defined and used in Section 327(1) and Section 342.2 of the *Criminal Code*.

Other Matters

45. While the Consultation focuses on acts that are intended to negatively impact critical infrastructure, the security of telecommunications infrastructure also faces serious threat from acts of theft and vandalism. Since January 2022 there have been hundreds of incidents of vandalism and theft across the country, many of which have negatively impacted the critical telecommunications infrastructure supporting emergency services, hospitals, governments, and financial services.
46. In many cases, the target of these crimes is the copper wires that form part of the network and that can be sold as scrap metal. While copper is the target, these acts often damage other parts of the network, including fiber optic cables.
47. In March 2023, the Canadian Telecommunications Network Resiliency Working Group (Resiliency Working Group), a sub-committee of the Canadian Security Telecommunications Advisory Committee (CSTAC) issued a report¹² in which it recommended that the federal government:

Create an article of federal law that specifically protects CTSP's [Canadian telecommunication service provider's] critical and ancillary infrastructure and maximizes criminal penalties in the event of willful or negligent damage to, and/or acts of vandalism or theft of critical network infrastructure.¹³
48. While these acts of vandalism and theft are typically not motivated by a desire to impair the operation of telecommunications networks or prejudice the national interest, criminals are aware, or ought to be aware, that their actions could have such an effect and they proceed despite this risk.
49. The potential negative impact of such acts is no less than those caused by acts which are intended to harm national security, and as the Resiliency Working Group recommends, Canada should implement stronger penalties for willful or negligent (or reckless) damage to, and/or acts of vandalism or theft of critical network infrastructure.
50. One way to do so is to create specific offences under the existing Criminal Code provisions for mischief and theft to specifically target acts against telecommunications, telecommunications facilities, and telecommunications services and to carry with them harsher sentences.¹⁴

¹² [Telecommunications Network Resiliency in Canada: A Path Forward](#), March 2023

¹³ Ibid. Section 1.2 – recommendation #1.

¹⁴ Draft provision (Theft):

333.2 Everyone who commits theft is, if the property stolen is all or part of a telecommunications facility, or intended to be used as all or part of a telecommunications facility, guilty of:

51. As an alternative to the creation of a specific offence of mischief targeting telecommunications facilities, the government could create a new offence against public order under Part II of the Criminal Code. The following draft provision aligns with the language found in s.77(e) of the Criminal Code which creates the offence of causing damage to or interfering with the operation of any air navigation facility where the damage is likely to endanger the safety of an aircraft in flight:
- (1) Everyone who causes damage to or interferes with a telecommunications facility where the damage or interference is likely to render the telecommunications facility incapable of providing or distributing telecommunications services is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.
52. While the Department of Justice may conclude that introducing new theft and mischief offences or creating a new offence against public order falls outside the scope of this consultation, we urge the department, together with other departments such as Public Safety, to recognize the risks to Canadians' safety and security posed by acts of vandalism and theft against critical telecommunications infrastructure, and to act on the recommendation of the Resiliency Working Group.
53. Furthermore, if such recommendation is considered to be outside the scope of this consultation, we note that Australia, as referenced in our response to question 2 above, includes as one of its sabotage offences an "Offence of sabotage reckless as to national security."¹⁵ A person is guilty of such offence if their conduct results in damage to public infrastructure and the person is reckless as to whether the conduct will prejudice Australia's national security. The creation of such an offence as a companion offence to other sabotage offences would provide additional deterrents against harmful activities that threaten the security of Canada's telecommunications networks.

Conclusion

54. The Canadian Telecommunications Association supports the premise of the Consultation that Canada should update the Criminal Code's law of sabotage. Foreign interference and the threat of domestic bad actors inflicting damage to Canada's critical infrastructure, such as telecommunications and broadcasting

-
- (a) an indictable offence and liable to imprisonment for a term of not more than fourteen years;
 (b) an offence punishable on summary conviction.

Draft provision (Mischief):

- 430(4.3) Everyone who commits mischief in relation to a telecommunications facility is guilty of:
- (a) an indictable offence and liable to imprisonment for a term not exceeding fourteen years;
 or
 (b) an offence punishable on summary conviction.

¹⁵ S.82.6

networks and related equipment, pose a serious threat to the safety and security of Canadians. As like-minded democracies such as the UK and Australia have done, updating the law of sabotage will send a powerful message of deterrence and strengthen the public's confidence in the government's efforts to protect the national interest.

55. For the same reason, we also urge the Government to introduce an article of federal law to protect critical infrastructure from wilful or negligent damage, vandalism or theft. The harm to Canadians that results from such acts and the concomitant impact on public confidence can be as serious as that which results from acts motivated by the intention to commit sabotage.

End of Document