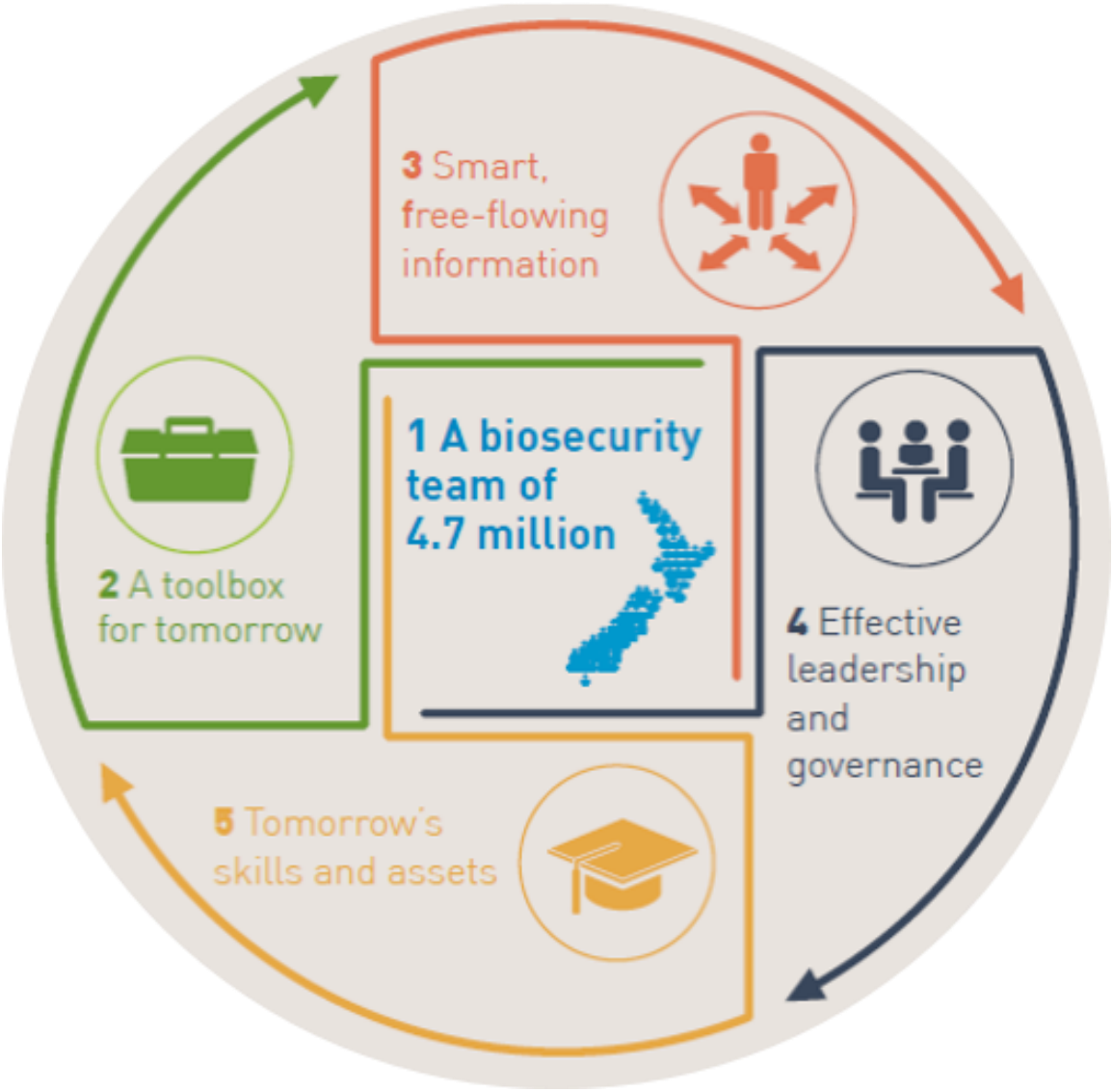
BIOSECURITY 2025



WORK PLAN

Strategic Direction 3

Smart, free-flowing information

Contents

1 Purpose of this document 3
2 Key messages from the SD3 Working Group 3
3 What success would look like 5
4 Actions to deliver the outcomes 10
5 Measures and targets 18
6 Links with other strategic directions 19
Appendix 1 – Glossary 20

Strategic Direction 3: Working Group Members

Ed Abraham, Dragonfly Data Science

Jamie Ataria, Cawthron Institue and Te Tira Whakamataki

Amanda Black, Lincoln University and Te Tira Whakamataki

Sophia Clark, Northland Regional Council

Andres Crofoot, Federated Farmers

Craig Davey, Horizons Regional Council

John Kean, AgResearch

Sam Leske, Ministry for Primary Industries

James Mansell, Noos LTD

Richard Palmer (Chair), Horticulture NZ

Waitangi Wood, Wai Communications Ltd and Te Tira Whakamataki

1 Purpose of this document

This outline work plan was produced by the Strategic Direction 3 Working Group, as its contribution to the Biosecurity 2025 implementation plan. The work plan sets out what the Working Group believes is needed to deliver the goals and outcomes for Strategic Direction 3. It has been produced to enable the Steering Group and other participants to consider it alongside the outline work plans, and undertake a process of rationalising and synthesising to create a final implementation plan.

2 Key messages from the SD3 Working Group

Trust is the core of data and information collection and sharing

This work plan adopts a trust and consent-based approach to data-sharing, in which data becomes a pooled community resource provided and accessed by a diverse group of participants. The contributors develop rules for use which facilitate sharing and transparency. This approach is called a 'data commons'. It can start with sharing and coordinating the standards for a few key datasets, and then gain momentum over time as potential participants see the demonstrated value of inclusion. The approach aims to build data-sharing communities, remove duplication of effort in the system, enable all participants to analyse data, and enable data reuse by building trust.

To gain and maintain trust this work plan seeks to:

- Return value to those who provide data
- Enable participants to control their own data
- Ensure sensitive information is appropriately secured
- Embark on a consensus-building process of data sharing
- Protect Māori data sovereignty and follow best practice for tikanga, especially for taonga species

Biosecurity system participants need to foster a culture of information sharing

To realise the value of data it must be readily found, accessed and integrated. Enabling this value to be realised will require a culture of information sharing. It means the default setting is that sharing information is the norm, and is built into attitudes, behaviours, rules and practices.

Innovation in data analysis is maximised when the analytical resource of diverse system participants can be brought to bear on an issue, rather than relying on a single system participant. So in addition to enabling information sharing, we need to support and encourage collaboration in the use of information. Fostering and curating a productive biosecurity data ecosystem is therefore a key goal of this work plan.

Two common issues for biosecurity data are integration and reuse

To have 'smart, free-flowing information' and to ensure biosecurity data can be effectively used for biosecurity risk management, there are two foundational processes which must be undertaken:

- Data is collected, stored and described in ways that enable it to be shared; this means standards are agreed on, and used consistently so that data drawn from different sources is comparable.
- People have assurance that if they provide access by others to their data, their rights, obligations, responsibilities and sensitivities about their data holdings will be acknowledged and protected; this means

***Data reuse** is when shared data is used for a new purpose – for something that was not intended when the data was first collected.*

protocols that ensure protection of those rights and obligations are built into any data sharing processes.

Two actions in this work plan to address these critical issues are to coordinate and drive the adoption of data standards, and to develop social protocols for data collection, access and reuse. Taken together, these actions should, over time, deliver a growing pool of easily integrated, searchable, and accessible datasets, and will support undertaking most of the other actions in this plan.

The initial steps to achieve this will be to reach agreement on what are the most important or significant data holdings for the biosecurity system, and what data standards and protocols should apply to them. Once these are agreed and put in place, the standards and protocols can be rolled out to other data holdings across the system. This will be a collaborative approach that will mean cooperation and trust are built through mutually agreed rules.

Smart, free-flowing data can drive better decision making before or at the start of an incursion

A large quantity of data and information that could be used to support better biosecurity decision making already exists, but it isn't used as effectively as it could be. This is because people who could use it don't know about it, it isn't easily integrated, or its access or use is restricted. Smart, free-flowing information will enable the analysis needed to better target resources toward prevention and early detection of incursions, through diverse and well curated datasets and information channels. As well as high-level decisions made by central government agencies, this data can inform the hundreds of decision makers in the broader biosecurity community to allocate their resources to greatest risk.

The global biosecurity context and resources need to inform and enable our biosecurity system

Many New Zealand biosecurity system participants maintain networks with their international counterparts. We want to ensure people know about and are enabled to better draw on these networks for biosecurity outcomes. To achieve this, this plan lays the groundwork for establishing an international biosecurity community, proposes mapping the existing relationships biosecurity participants have with international partners to help facilitate new connections, and provides support to integrate important domestic and international datasets.

Additionally, there is a growing potential for international data and information to support New Zealand's biosecurity system through data analysis and intelligence. A broad, multidisciplinary approach to international data analysis through a 'biosecurity situational awareness and intelligence warning system' is proposed in this work plan. This will integrate and build on existing systems to:

- Identify global biosecurity trends and predict their impacts
- More precisely target biosecurity risk
- Draw on social, economic, environmental and other data sources to support the early detection of pest and disease threats overseas

3 What success would look like

GOAL 1: Accessibility

Information is shared and open wherever possible.

OUTCOME	What success would look like
System-wide priorities Information needs are understood at a system-wide level. Priorities are set strategically across the system.	The biosecurity system has clearly set out priorities for information needs. Biosecurity system participants know what information is needed and why.
Key data sources The fundamental datasets required to support effective decision making across the system are known. Data is collected, maintained and stored using agreed consistent standards to support easy sharing of data.	Key data will be identified and maintained. Key data conforms to agreed data standards. Participants know how to collect data correctly (because there are protocols and procedures that they know about and/or it is built into the collection method). Mātauranga Māori concepts are incorporated into relevant data standards. *Commentary: The need for consistent data standards, used throughout the sector, and in line with international standards, is one of two cornerstones on which this goal is based. Standards need to be sufficiently flexible to accommodate local (NZ) requirements and be updated. It is acknowledged that some key data sources will be generated outside the biosecurity system.*
Distribution of Access Information is regarded as a system-wide asset, available to all who can make effective use of it, regardless of who collected or holds it.	Participants act as collective curators of data. Participants that want to share information will, because they see value in sharing and trust the custodians. Data will be used by a wide range of biosecurity system participants to advance biosecurity. *Commentary: While our overall direction is trending to open information sharing, with benefits for many parties, there are some situations where data owners do not want to share, for cultural, privacy or commercial reasons. In these cases, we would like the data owners to make it known that the information exists, and be open to being engaged in a discussion about how information could be used for biosecurity purposes, within agreed access protocols.*
Supporting Mobility Workers are able to record biosecurity information from wherever they may be working, and are able to access centrally-	Data will be collected once (there is no duplication of recording or transcription). Practitioners in the field have access to the information they need.

held information from remote locations.	*Commentary: Mobility requires hardware and tools that support remote working, but we can only take advantage of this if we create an information environment that allows people to build tools. The first three outcomes of this goal are required to create this environment.*

Commentary: Accessible information is both available and is able to be understood by all potential users. The key words associated with this goal are therefore TRUST and STANDARDS – accessibility will flow from these.

This goal will only be achieved where there is trust – of both the data custodians and the system participants that use information – so that data contributors are willing to provide information, rather than holding it in a traditional ownership model. It was acknowledged that there will be situations where participants will want to retain control of their data, and this is especially true of Mātauranga Māori. However, the Working Group expects that, over time, there will be a paradigm shift to a presumption of sharing information, within agreed access protocols.

The need for consistent data standards, used throughout the sector, is the second cornerstone on which this goal (and whole strategic direction) is predicated. Collecting data once, correctly ("do it once and do it right") was identified as one of the most important success factors by the Working Group. This has been split into two success factors in the above table – related to standards and mobility. Collecting data once, correctly, will occur where we have agreed standards, so that users know what data and metadata are required, in what format, using consistent vocabulary. An outcome of this is that we will have more usable data (which will be able to be shared). To support mobility, workers in remote locations need to either know the standards and protocols for data collection before they go into the field, or have access to it in the field (for example when recording results directly into a database or app), to ensure data is collected once, correctly, and so minimise errors and the need for transcribing data.

Open-sourcing validation is seen as a major benefit accruing from the concept of collective curation – the fact that data will be viewed by many parties, who can all contribute to validating the data. Other measures of success will be increased collaboration between organisations, and opportunities for collaboration and innovative uses.

GOAL 2: Effective Use

We unlock the full value of information through the best data use and analysis.

Commentary: The Working Group re-ordered the outcomes in the Direction Statement to reflect a logical order of input-analysis-output. That is, if we (1) have data from diverse sources available to the biosecurity community, and (2) that community is able to reliably interpret it through analysis, then (3) this will support the community to be situationally aware.

OUTCOME	What success would look like
Networked sensors Biosecurity risk management is more effective through the use of big data such as that generated by networked sensors, e.g. in environmental locations by industry or local government, monitored and analysed by automated systems, with users notified if intervention or response is necessary.	Data from a diverse variety of sources can be easily utilised for biosecurity purposes. *Commentary: Networked sensors or big data are some of the sources of data, and it is likely that the proportion of data used for biosecurity purposes that is generated from these sources will increase over time. This will speed up the collection of data, and may speed up any subsequent response. However, this will only occur if the data from these is accessible. So, successful realisation of this outcome requires accessibility. The Working Group considers that this outcome will be enabled by the actions in Goal 1, and will flow naturally as technology develops. It was not considered necessary to prescribe what type or how many sensors should or shouldn't be used.*
Analytics The best analytics are employed to turn data into information and intelligence for risk assessment, and to ensure resources are allocated to the areas of highest need.	Data is presented clearly, understood, and applied correctly for decision-making. Data users understand the context in which biosecurity data is collected, so that it can be used appropriately for analysis (e.g. through metadata standards). Data can be used by a wide range of biosecurity system participants for disparate analytical purposes (including human health impact analysis). *Commentary: Analysis is carried out by computers or algorithms, but also by human interpretation; remember that connected people are often the best network of sensors. Availability of metadata is crucial information for those doing analysis.*

Situational Awareness

Information supports widespread understanding of biosecurity risks, coordinated effort, better decision-making at all levels across the system, and enhanced participation.

Information is available for all biosecurity system participants to inform critical biosecurity decisions.

Decision-making is transparent because everyone involved can see the information on which decisions are based.

Participants respond more quickly, so decisions can be made closer to the beginning of the invasion curve.

Participants take part because they can contribute to and access information.

Participants are invested because they understand the risks and threats.

Commentary: Accessible data needs to be usable and understandable in order to be used effectively.

- Improved accessibility would facilitate better decisions to be made earlier (e.g. earlier in an invasion/response situation), as long as the right data is available to inform the decision.
- Improved ability to take part will result in a wider range of users, potentially for quite disparate purposes, resulting in potential for greater innovation.

Both improved accessibility and more effective use should lead to more transparent decision-making (e.g. of where to invest in control, when to strive for eradication). This was identified as one of the most important success factors by many of the Working Group, who felt that system participants should be making decisions in partnership – with each other and decision makers.

Information enables dialogue – therefore, one of the outcomes of this strategic direction will be to enable conversations and information sharing, which will in turn lead to ideas for new tools and new approaches.

GOAL 3: Preparing for the future

We anticipate and take advantage of the ways that information technology will transform society, support participation, and enhance biosecurity effectiveness.

OUTCOME	What success would look like
Anticipate the future Preparation for the transformational aspects of information technology becomes a standard part of biosecurity system planning and thinking.	Data standards will accommodate diverse and distributed data sets. Information systems will be affordable, scalable and adaptable. Diverse users and interested parties are around the table during the design process of the data system.
Take advantage of opportunities Action is taken to make effective use of emerging information technologies, and to mitigate the risks that may emerge through the transformation of business practices and society behaviours.	Leadership responds quickly to change and new opportunities. A skilled workforce responds to changes in technology, to identify opportunities and adapt processes. *Commentary: If we succeed, we will have an open market in innovation and no missed opportunities.*

Commentary: The main themes of this goal are the need for agility and the creation of a data ecosystem that all participants can plug into, and share information across. We can achieve these outcomes by making the building blocks (from Goal 1) flexible, and ensuring we have the social license to share data and information. The sharing of information will require system participants to act as collective curators (of information), and this is expected to let innovation in.

4 Actions to deliver the outcomes

Fundamental Establishment Actions

This first cluster of actions is focused on delivering a biosecurity 'data commons' to improve the way biosecurity system participants share and use data. It is a process of engagement between participants, working to identify common interests in data sharing, and overcoming technical and trust-based barriers to sharing. A significant component of this is developing common standards for data, and agreements on use and access. Ultimately this results in pools of data which (if participants agree) can be easily found, accessed, integrated and reused.

1. **Establish an information advisory group** for the biosecurity system, to provide ongoing oversight and review of the biosecurity data ecosystem, thought leadership, and to steward the implementation of the actions in this plan and the vision for 2025.
   The information advisory group will:
   - Be responsible for leading the biosecurity sector on trust and social licence issues, with respect to data and information
   - Champion free-flowing data, including supporting legislative and regulatory systems that support open data sharing for biosecurity
   - Be committed to the principles of the data commons and follow best-practice guidelines (as developed in Action 8)

   Specific tasks for the group will include: coordinating the identification of data needs and priorities (Action 2), the adoption of data standards for the biosecurity system (Action 3), and social protocols for biosecurity data (Action 4).

   The group should have appropriate Māori representation to provide perspective, particularly of developing and accessing traditional knowledge and data (mātauranga). Special focus should be paid to:

   - Protecting Māori traditional knowledge, culture, and data sovereignty
   - Ensure cultural context of data is incorporated in data standards (e.g. organism whakapapa, Mātauranga metadata)
   - The interconnectedness of people and the environment (e.g. in identifying biosecurity outcomes including human health and culture)

   The group's structure could comprise an advisory group, with more technical sub-groups as required, e.g. for data standards and information sharing protocols. Membership should be dynamic, to respond to fast-moving technological changes.

2. **Identify the data needs and priorities of the biosecurity system**. This should begin with quickly identifying a few areas in which to begin developing data standards and use protocols (Action 3 and 4). These may be based on:
   - The early identification of work currently progressing in the creation of data standards for biosecurity (see Action 3)
   - The priorities in other Biosecurity 2025 work plans requiring data and intelligence
   - Priorities articulated by the steering group such as cross-cutting issues

   This initial-needs analysis should quickly identify areas of focus, to deliver value and kick-start the data commons.

Secondly, there should be a broader analysis of all information needs and priorities of biosecurity system participants. The process should focus on identifying data and information problems. This may be achieved by:

- Wide scale consultation with the biosecurity community, to identify problems relevant to data and information
- Identifying nationally significant data sets and key data requirements that need to be developed or provided with ongoing support (to be maintained, updated and accessible)
- Identifying Mātauranga Māori (traditional Maori knowledge and information) assets in this process
- Identifying opportunities for existing useful information to be made available in standardised form to the biosecurity community, where currently it is not
- Mapping the information communication channels and procedures for key biosecurity activity across the system, especially for time-sensitive operational information. This means that relevant system participants receive up-to-date information when they need it
- Paying special attention to marine and human health biosecurity information needs

This process is critical for identifying and making use of data for the biosecurity system. However, all types of information are in scope for this broader information needs analysis.

3. **Coordinate and drive the adoption of data and metadata standards** for biosecurity data, beginning with the priority data issues identified in Action 2. This programme of work will require wide-reaching coordination within the biosecurity community. It will enable the efficient integration of key datasets across the biosecurity system. This is a modular process which will start with a single data issue (e.g. creating common data standards for how a location is recorded by biosecurity system participants) and then build momentum over time.

   There are several key principals this work is based on:

   - A great deal of work on common standards is already being undertaken, and this process should identify, drive and expand this work where possible (e.g. MPI biosecurity common data standards, NZOR).
   - All standards need to be consistent with international best practice to ensure international data can be easily on-boarded.
   - Mechanisms should be incorporated from the start to easily modify standards to adapt to changing needs.
   - Metadata standards should include direction on storage and retention of samples, and information on access and reuse.

   ***Data standards** are ways of organising and describing data so it can be easily integrated and used. For example for two people to share data on 'pest distribution' they need a shared understanding of what a pest is, a consistent name for each pest, and if they are using locations then they need a consistent way of describing them, such as addresses or latitude and longitude.*

   This work should in time develop a 'data commons' for biosecurity, in which system participants conceptualise data as a resource to be shared and used as efficiently and openly

as possible. This is enabled through the standards (in this action) and use protocols (in Action 4).

4. **Develop social, cultural and technical protocols for data collection, access and reuse** for different communities of users. This should follow the data commons approach to gain and maintain trust. As part of this process, agreed rules will be developed which ensure a sustainable model of data use (e.g. rules on who can use my data and for what purpose).

   > ***Data use protocols*** *are rules for how data can be accessed, used, reused and secured. At its most basic level this may be a formal agreement between parties, or a creative commons licence agreement.*

   This process should incorporate the following:

   - Acknowledgement and integration of the role and traditions of Mātauranga Māori (traditional Maori knowledge and information) in data ownership, provision and use
   - Recognition that data contributors want to see some return of value for their cooperation (e.g. by having access to information gained from the data)
   - Publicly-funded biosecurity data and information should be made available to the biosecurity community when possible

   As a part of this process there should be a **review of the legislative or regulatory data sharing environment**, to ensure it is fit for purpose in achieving the outcomes of the biosecurity strategy. This should include an analysis of existing information sharing arrangements between biosecurity system participants, to ensure that the sum of information sharing arrangements are fit for purpose from a system-wide perspective.

High-impact actions and key strategy deliverables

These actions are all critical for delivering the outcomes and targets specified in the Biosecurity 2025 Direction Statement. They are more tangible and less process-based than the 'Fundamental Establishment Actions' listed above, but they are largely based on those establishment actions occurring.

5. **Provide biosecurity data and information to the biosecurity community through an integrated environment.**
   Data and information generated by biosecurity system participants, programmes, and other activities (e.g. surveillance, response operations, and pest distribution information), should be accessible in an easily usable, spatially-enabled format to relevant biosecurity community participants. As well as providing data, this action will provide the tools and resources for system participants to process, analyse and interpret data (this is because not all system participants have the resources and capability to process and analyse data).

   A key SD3 principle is that information sharing should be a default position, especially information owned or funded by government agencies. This means information should be shared even when there is no immediately obvious or demonstrated value to others in the system. This is part of the SD3 goal of preparing for future innovations in which data may provide unintended value to unexpected participants, and therefore a diverse data ecosystem is desirable. Where information cannot be shared (e.g. due to privacy, national interest, or commercial sensitivity), efforts should be made to mitigate these risks. Priorities for which information should be made available first, and how it should be delivered, will be identified in the needs analysis in Action 2. As a guideline it may include data and information on:

   - Surveillance programmes
   - Operational activities and decision making (e.g. all relevant biosecurity system participants should understand when and how a decision is being made, and be able to access the information the decision is based on)
   - Organism status and distribution (e.g. how a pest is being managed)
   - Contextual organism information (e.g. potential distribution, specific industries at risk)
   - Evidence-based risk assessments that consider human health impacts

   The integrated environment should be open to relevant biosecurity system participants, and easy for them to use. Examples of possible features include:

   - For each organism, provide summary status and risk information, so that people can get a quick overview or synopsis of where it is, what we know, why it's a risk and what we are doing about it – including whether we are responding or managing
   - An interactive map of pest and disease distribution, surveillance activity, and operational activity
   - Where a response plan is in place, details of plan to be provided (including risk assessment, actions, organisations involved, decision making process)
   - Ultimately expand this to include border interception data

6. **Create a biosecurity situational awareness and intelligence warning system** which builds on existing systems. This system will analyse offshore data and information to help identify and manage threats. Outputs will be accessible to relevant

participants in the biosecurity system where appropriate. Key contributors into this system would be:

- MPI's existing Emerging Risks System (ERS), which should be developed to provide push notifications on risk analysis to relevant members of the biosecurity community (outputs from this system will also feed back into the ERS for risk assessment)
- A biosecurity data analytics function which is able to examine relevant data sets to identify trends and assess risks
- Proactive development of international information-sharing agreements, to ensure international governmental data is able to feed into the system
- An open-source media, academic, and social media scraping programme. to generate data for analysis of global events and trends
- The international industry and practitioner networks developed in Action 11
- Analysis of other countries' biosecurity systems and policies

This system must be able to look at strategic threats (e.g. long term trends) and take a broad, multidisciplinary approach to analysing threats and risks. A searchable environment should be provided in which participants can locate information on biosecurity risks, and where subscribers are able to check the status of a possible threat through the analysis process. The risk assessment and underlying data should be visible to the biosecurity community, making biosecurity decision-making more transparent to all participants.

7. **Ensure the development, adoption and utilisation of the New Zealand Organisms Register (NZOR)** as the national database for biological data, based on agreed data standards developed and maintained by the Bio Data Infrastructure Group (BDI).

   Biological data comprise one of the biosecurity data components. The NZ Organisms Register is a federated database for biological data (used for more than just biosecurity purposes). This structure is already established and has been supported by MPI, DOC and the Ministry for the Environment, but no long term funding or MOU is in place. This action requires a budget to fund and develop NZOR for the long term.

   Other actions in this plan (e.g. the needs analysis in Action 2) may necessitate the NZOR is further developed and built upon over time. NZOR is able to be adapted to the needs of biosecurity participants and therefore this should not present an obstacle to implementation.

8. **Develop proof-of-concept models and guidelines for supporting the biosecurity data commons.** This is to help others contribute to the data commons, and also to help explain the data commons value proposition. This should include developing exemplary non-proprietary social, data and technical architecture standards for several suitable datasets (i.e. take two or three datasets through the processes described in Actions 3 and 4, and develop guidelines for others to replicate these processes). This should model best practice and provide a proof of concept for the data commons. Additionally, capturing stories behind how these initial datasets were used, and the processes that they went through, will be critical for demonstrating value and building momentum in the data commons.

9. **Ensure the system is innovative and makes best use of new generations of data tools**. This should include:
    - A mechanism for regularly scanning for technology changes that would have implications for the biosecurity system, and feeding into the Information Advisory Group (in Action 1) and to governance bodies as appropriate for review and response
    - A function for identifying and recommending measures to overcome blocks to innovation in data analysis, collection tools (e.g. networked sensors), and data sharing, to support the 'fundamental establishment actions' (Actions 1, 2, 3 and 4).
    - Highlighting novel and valuable uses of data analytics for biosecurity outcomes, and where possible supporting other biosecurity system participants to replicate and build upon this analysis.

Expanding capability and growing networks

These actions are focused on the long term activity of fostering the biosecurity data ecosystem, through community building and adopting new technologies and data practices.

10. **Develop a Biosecurity Information Community**
    Establish forums and channels for practitioners to promote and enable discussion and share information. This may include subgroups, e.g. for emerging threats, data standards, reuse protocols, responses, pathways etc. SD3 Working Group members should be champions for this community.

    The purpose of this action is to link data and information stakeholders in the biosecurity system. Resources need to be dedicated to enable a person or group to curate this community. One of the aims of the community should be to leverage off the international biosecurity data and information linkages described in Action 11.

11. **Build and coordinate international biosecurity data and information linkages**. Many parts of the New Zealand biosecurity community maintain strong international relationships with their overseas counterparts. These networks should be supported and developed, to contribute to New Zealand and global biosecurity outcomes. Steps should include:

    - Mapping the landscape of existing international connections. Provide this as a resource to the biosecurity community. Identify valuable information and data held by international partners that may contribute to NZ's biosecurity system.
    - Identifying obstacles to and opportunities for developing and improving linkages to key overseas entities
    - Supporting the development of international information-sharing agreements, for high-priority information and data.
    - Providing support to integrate international data standards into the domestic common standards work (Action 3) where possible. We should also champion and support the adoption of NZ domestic standards by the international community when appropriate.
    - Starting initial steps to create an international biosecurity community by curating international communication and collaboration tools (e.g. online biosecurity fora, social media groups) most likely using existing platforms.

12. **Ensure the biosecurity system has the data, skills and assets needed to support an advanced data analysis function.** This function should support predictive models and network analytics, for understanding existing and future biosecurity threats and opportunities. It also should inform risk assessment, the development of import health standards, and feed into the situational awareness and intelligence warning system in Action 6. System participants should identify opportunities for improving data analysis capabilities and coordination, and propose strategic investment in this function where appropriate.

13. **Develop best-practice guidelines for coordinated community activity in biosecurity**
    Consider developing a lay-person implementation guide to data standards and information sharing protocols, targeted at community groups, to ensure that data collected can be understood across the system. This action can be looked at in the medium to long term, as

there is potential for development of tools that will improve the quality of data capture (e.g. apps may capture a lot of the data and metadata in a standard form).

14. **Identify funding opportunities for innovative biosecurity data technology projects**. Helping to fund the rapid assessment and development of tools and technologies may contribute to biosecurity priorities. The programme will identify information and data management options that could be suitable for funding new approaches to biosecurity data and analysis. It should be based on the needs analysis undertaken in Action 2.
15. Identify opportunities to **collect new data from networked sensors** as they arise (e.g. in environmental locations by industry or local government, monitored and analysed by automated systems). As well as helping to overcome roadblocks to the use of networked sensors, this will enable the development of regional networks of distributed sensors and other regional biosecurity data collection systems. This should be based on the needs analysis undertaken in Action 2.

5 Measures and targets

2025 Targets listed in the Direction Statement:

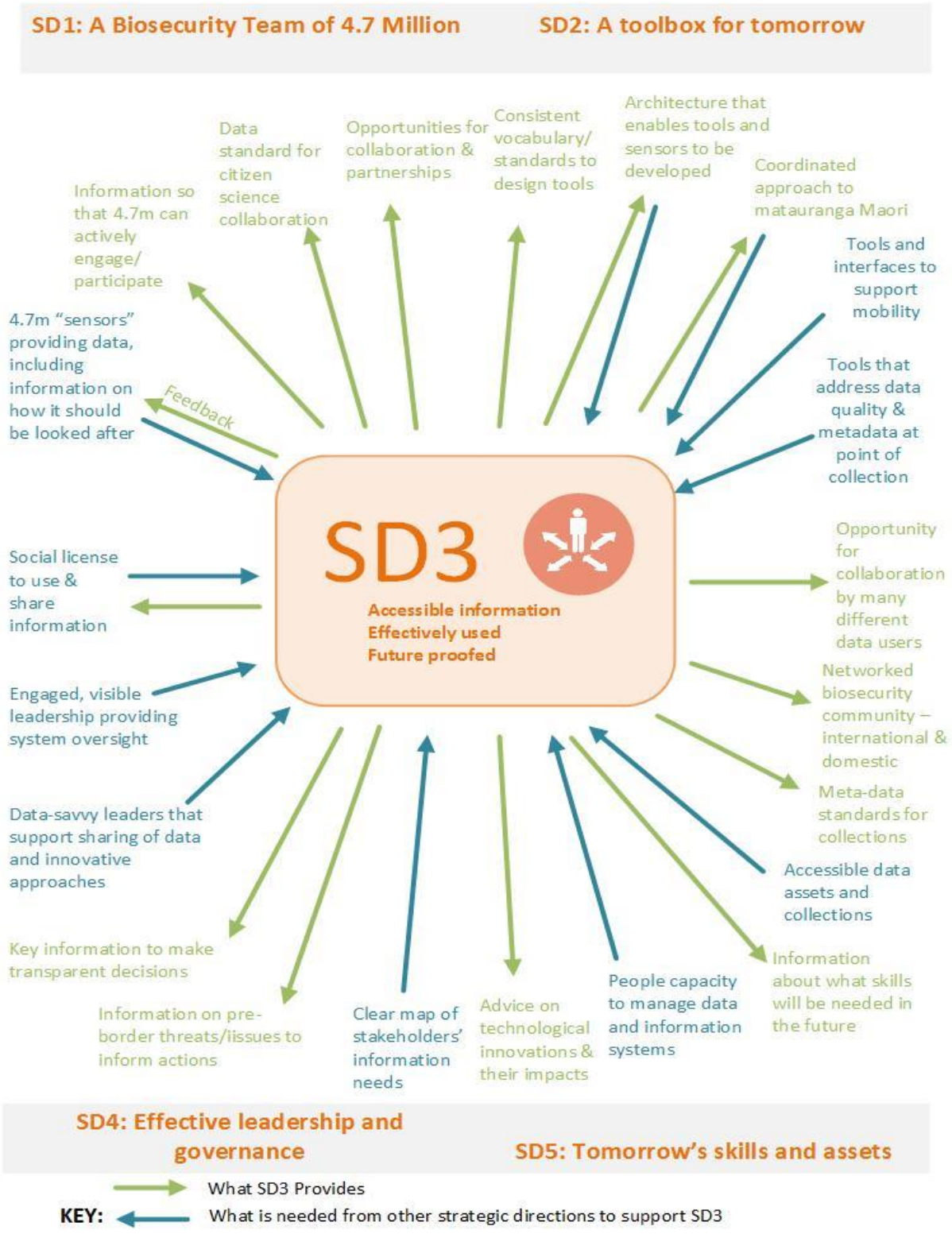
1. A publicly-accessible network enables electronic access to organism data held by central government agencies, regional councils and Crown research institutes.
   Organism data, linked together from multiple sources and including information on species name, distribution and impact, is crucial to identify and manage biosecurity risks.
2. Automated and targeted alerts about emerging risks are available to all participants across the biosecurity system.

These targets will be met through the actions described in this work plan. The working group proposed an additional target which better reflects the ambition and scope of the work plan.

“Key data sets for targeting early biosecurity interventions have been identified, and 80% of this data is available to system participants through an agile data sharing system.”

6 Links with other strategic directions

There are various interdependencies between the strategic directions. The diagram below maps out key outputs from other strategic directions to SD3 and vice versa.



Appendix 1 – Glossary

Data Commons – A concept for community-based data management, which supports inclusion and data reuse (i.e. using data for a different purpose from which it was originally intended). A commons-based approach requires community agreed standards, protocols and a high degree of trust between users and providers of data.

Data Ecosystem – The total system of people, practices and technologies supporting a data community of practice (in this case, the biosecurity community). This includes data management, data custodianship and curation policies, legal frameworks or procedures to execute those policies and manage data, data standards, a data governance framework and organisational structure, and the technology platforms that store and link data.

Data Reuse – Using data for a different purpose than for what it was originally collected. This reuse may be by the original user of the data, or by a different party with whom the data was shared.

Data Standard – Agreed standards for data collection, storage, security, dissemination and usage, including standards for metadata. Data standards may be developed alongside social standards for how the data is used, managing issues such as privacy, data reuse, and ownership.

Distributed Ledger – A method for how a set of data is stored. It can be thought of as a database held on everyone's computers that is constantly synchronised across a network. When information is updated in a data set, everyone connected immediately receives that update, enabling constant reconciliation.

Federated Database – Multiple databases connected together. When a user searches for data on a federated database, the system will reach back through its constituent databases and return the relevant data.

Internet of Things – A network of physical objects (such as household items, vehicles, environmental monitors) that contain embedded technology that gathers data and streams it over the internet, where it can be analysed and processed.

Metadata – Information that describes the data set – for example, how, when and by whom a particular set of data was collected, how the data is formatted, and administrative aspects (including access). Metadata is most useful when it is provided in a standardised, structured way to make it easily comparable and searchable across data sets, and it is key to providing context for analysis.

Networked Sensors – Devices capable of collecting data and sending it through a network to be analysed. As networked devices become cheaper, a growth in data provided through these sensors is expected, which has implications for a range of environmental reporting.