```
module ietf-dots-signal-control {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-dots-signal-control";
  prefix dots-control;

  import ietf-dots-signal-channel {
    prefix ietf-signal;
    ~~reference~~
~~      "RFC 8782: Distributed Denial-of-Service Open Threat~~
~~                 Signaling (DOTS) Signal Channel Specification";~~
  }
  import ietf-dots-data-channel {
    prefix ietf-data;
    reference
      "RFC 8783: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) Data Channel Specification";
  }
  import ietf-yang-structure-ext {
    prefix sx;
    reference
      "RFC 8791: YANG Data Structure Extensions";
  }

  organization
    "IETF DDoS Open Threat Signaling (DOTS) Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/dots/>
     WG List:  <mailto:dots@ietf.org>

     Author:  Kaname Nishizuka
              <mailto:kaname@nttv6.jp>

     Author:  Mohamed Boucadair
              <mailto:mohamed.boucadair@orange.com>

     Author:  Konda, Tirumaleswar Reddy
              <mailto:TirumaleswarReddy_Konda@McAfee.com>

     Author:  Takahiko Nagata
                 <mailto:nagata@lepidum.co.jp>";
  description
    "This module contains YANG definition for the signaling
     messages exchanged between a DOTS client and a DOTS server
     to control, by means of the DOTS signal channel, filtering
     rules configured using the DOTS data channel.

     Copyright (c) 2020 IETF Trust and the persons identified as
     authors of the code.  All rights reserved.

     Redistribution and use in source and binary forms, with or
     without modification, is permitted pursuant to, and subject
     to the license terms contained in, the Simplified BSD License
     set forth in Section 4.c of the IETF Trust's Legal Provisions
     Relating to IETF Documents
     (http://trustee.ietf.org/license-info).

     This version of this YANG module is part of RFC XXXX; see
     the RFC itself for full legal notices.";

  revision ~~2019-05-13~~ 2020-07-07 {
    description
      "Initial revision.";
    reference
      "RFC XXXX: Controlling Filtering Rules Using Distributed
                 Denial-of-Service Open Threat Signaling (DOTS)
                 Signal Channel";
  }

  ~~feature control-filtering {~~
~~    description~~
~~      "This feature means that the DOTS signal channel is able~~
~~       to manage the filtering rules created by the same DOTS~~
~~       client using the DOTS data channel.";~~
~~  }~~

~~  augment~~
  sx:augment-structure "/ietf-signal:dots-signal/ietf-signal:message-type"
                     + "/ietf-signal:mitigation-scope/ietf-signal:scope" {
    ~~if-feature "control-filtering";~~
    description
      "ACL name and activation type.";
    list acl-list {
      key "acl-name";
      description
        "List of ACLs as defined using the DOTS data
         channel. ACLs bound to a DOTS client are uniquely
         identified by a name.";
      leaf acl-name {
        type leafref {
          path "/ietf-data:dots-data/ietf-data:dots-client"
             + "/ietf-data:acls/ietf-data:acl/ietf-data:name";
        }
        description
          "Reference to the ACL name bound to a DOTS client.";
      }
      leaf activation-type {
        type ietf-data:activation-type;
        default "activate-when-mitigating";
        description
          "Sets the activation type of an ACL.";
      }
    }
  }
}
```